

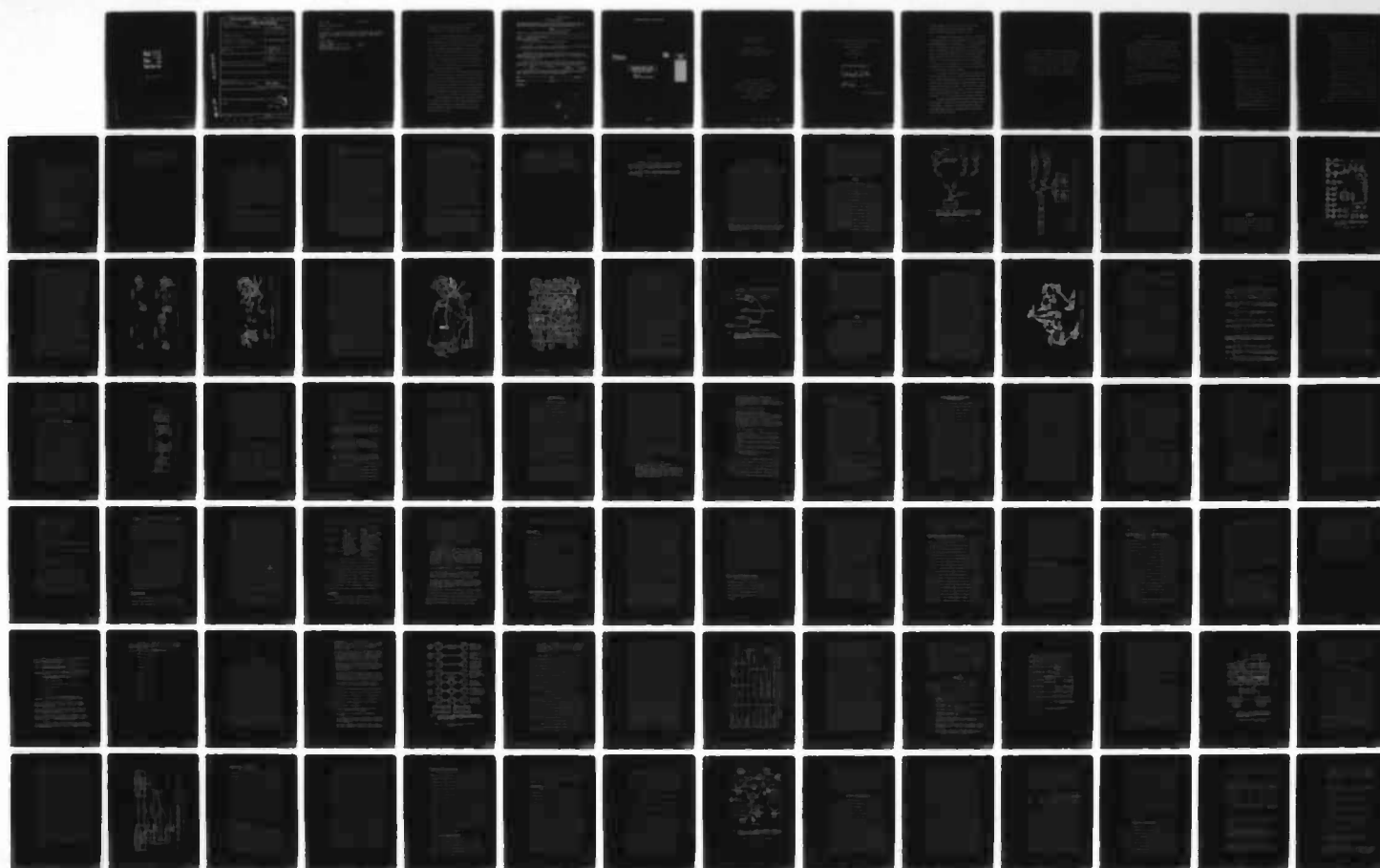
AD-A139 162

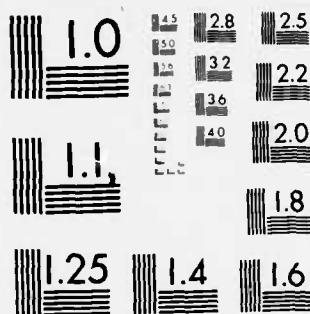
A PRACTICAL TERRESTRIAL PACKET RADIO NETWORK(U) AIR
FORCE INST OF TECH WRIGHT-PATTERSON AFB OH
S W PHILLIPS NOV 83 AFIT/CI/NR-83-83T

1/2

UNCLASSIFIED

F/G 17/2.1 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

UNCLASS

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER AFIT/CI/NR 83-001	2. GOVT ACCESSION NO. AD-A139162	3. REPORTING CATALOG NUMBER
4. TITLE (and Subtitle) A Practical Terrestrial Packet Radio Network		5. TYPE OF REPORT & PERIOD COVERED THESIS/DISSERTATION
7. AUTHOR(s) Samuel W. Phillips, III		6. PERFORMING ORG. REPORT NUMBER
9. PERFORMING ORGANIZATION NAME AND ADDRESS AFIT STUDENT AT: University of Colorado		8. CONTRACT OR GRANT NUMBER(s)
11. CONTROLLING OFFICE NAME AND ADDRESS AFIT/NR WPAFB OH 45433		10. PROGRAM ELEMENT PROJECT, TASK AREA & WORK UNIT NUMBERS
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		12. REPORT DATE November 1983
		13. NUMBER OF PAGES 128
		15. SECURITY CLASS. (of this report) UNCLASS
		16. DECLASSIFICATION DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES APPROVED FOR PUBLIC RELEASE: IAW AFR 190-17 13 Feb 1987 LYNN E. WOLAVER Dean for Research and Professional Development		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number)		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) ATTACHED		

AD A 139162

DTIC FILE COPY

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASS

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

84 03 19 103

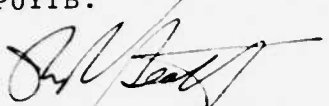
FROM: CIRS

22 Dec 1983

SUBJECT: Student Thesis

TO: AFIT/NR

Attached is the thesis of Capt Samuel W. Phillips III. Captain Phillips is a December 1983 graduate of the MS Telecommunications Program at the University of Colorado (Boulder). MAF Code is P0YTB.



THOMAS R. BEATTY, Major, USAF
Program Manager
Regular/Special Programs Division
Civilian Institution Programs

1 Atch
Thesis

Phillips, Samuel W. III (M.S., Telecommunications)

A Practical Terrestrial Packet Radio Network

Thesis directed by Professor Samuel W. Maley

A terrestrial packet radio network, now a competitive reality, offers a new alternative for local networks. Taking advantage of its adaptability to local environments and to the growing sources of digital communications, permits extension of data communications to remote locations. While adding capabilities for dispersed computer communications, there are limitations in using packet radio due to its bursty nature and less than absolute reliability. But as a message service for short duration communications, terrestrial packet radio may rapidly fill an important gap in communications.

This thesis examines the features and design considerations for a practical terrestrial packet radio network. Packet radio equipment, evolving through stages of sophistication and new generation microcircuitry, is approaching the hand held model. While new digital features improve its mobility, the crucial consideration becomes the interconnection with other systems through adaptable protocols. This issue dominates the current research.

Several terrestrial packet radio network testbeds exist under the direction of the Advanced Research Projects Agency. Networks, evolving since 1973, are now reaching stages for major implementation, and provide the basis for this study.

AFIT RESEARCH ASSESSMENT

The purpose of this questionnaire is to ascertain the value and/or contribution of research accomplished by students or faculty of the Air Force Institute of Technology (ATC). It would be greatly appreciated if you would complete the following questionnaire and return it to:

AFIT/NR
Wright-Patterson AFB OH 45433

RESEARCH TITLE: A Practical Terrestrial Packet Radio Network

AUTHOR: Samuel W. Phillips, III

RESEARCH ASSESSMENT QUESTIONS:

1. Did this research contribute to a current Air Force project?
☐ a. YES ☐ b. NO
2. Do you believe this research topic is significant enough that it would have been researched (or contracted) by your organization or another agency if AFIT had not?
☐ a. YES ☐ b. NO
3. The benefits of AFIT research can often be expressed by the equivalent value that your agency achieved/received by virtue of AFIT performing the research. Can you estimate what this research would have cost if it had been accomplished under contract or if it had been done in-house in terms of manpower and/or dollars?
☐ a. MAN-YEARS ☐ b. \$
4. Often it is not possible to attach equivalent dollar values to research, although the results of the research may, in fact, be important. Whether or not you were able to establish an equivalent value for this research (3. above), what is your estimate of its significance?
☐ a. HIGHLY SIGNIFICANT ☐ b. SIGNIFICANT ☐ c. SLIGHTLY SIGNIFICANT ☐ d. OF NO SIGNIFICANCE
5. AFIT welcomes any further comments you may have on the above questions, or any additional details concerning the current application, future potential, or other value of this research. Please use the bottom part of this questionnaire for your statement(s).

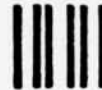
NAME	GRADE	POSITION
ORGANIZATION	LOCATION	

STATEMENT(s):



FOLD DOWN ON OUTSIDE - SEAL WITH TAPE

AFIT/NR
WRIGHT-PATTERSON AFB OH 45433
OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 73236 WASHINGTON D.C.

POSTAGE WILL BE PAID BY ADDRESSEE

AFIT/ DAA
Wright-Patterson AFB OH 45433



FOLD IN

83

A PRACTICAL TERRESTRIAL
PACKET RADIO NETWORK

by

Samuel W. Phillips III

B.S., Virginia Military Institute, 1975

M.S., Boston University, 1981

A thesis submitted to the
Faculty of the Graduate School of the
University of Colorado in partial fulfillment
of the requirements for the degree of
Master of Science
Program in Telecommunications
1983

84 03 19 103

This thesis for the Master of Science degree by

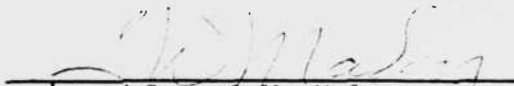
Samuel W. Phillips III

has been approved for the

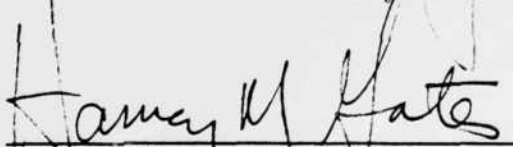
Program in

Telecommunications


by



Samuel W. Maley



Harvey M. Gates



John E. Hershey

Date 30 Nov. 1923

Phillips, Samuel W. III (M.S., Telecommunications)

A Practical Terrestrial Packet Radio Network

Thesis directed by Professor Samuel W. Mailey

A terrestrial packet radio network, now a competitive reality, offers a new alternative for local networks. Taking advantage of its adaptability to local environments and to the growing sources of digital communications, permits extension of data communications to remote locations. While adding capabilities for dispersed computer communications, there are limitations in using packet radio due to its bursty nature and less than absolute reliability. But as a message service for short duration communications, terrestrial packet radio may rapidly fill an important gap in communications.

This thesis examines the features and design considerations for a practical terrestrial packet radio network. Packet radio equipment, evolving through stages of sophistication and new generation microcircuitry, is approaching the hand held model. While new digital features improve its mobility, the crucial consideration becomes the interconnection with other systems through adaptable protocols. This issue dominates the current research.

Several terrestrial packet radio network testbeds exist under the direction of the Advanced Research Projects Agency. Networks, evolving since 1973, are now reaching stages for major implementation, and provide the basis for this study.

To my wife Jacqueline and my children Samuel, Julia and Sarah. I dedicate this book. All the studying in the world would not have been sufficient to complete this assignment without the love of my family. Life is too short not to be fulfilled by the taking of a wife and the warmth of a child's embrace. For this gift I am thankful, and for the support they have given me, I am overwhelmed. In deepest love I say thank you.

ACKNOWLEDGEMENTS

I am extremely grateful to the United States Air Force for this opportunity to advance my skills and knowledge in my field of expertise. The time I have spent gaining new insight into telecommunications I hope to repay in dedicated service to my country. For everything I have learned, the Air Force can be sure it will be applied with utmost diligence and care.

I wish to thank the members of my thesis committee: Professors Harvey Gates, Samuel Maley and John Hershey.

For her empathy and caring I also want to thank Mrs. Esther Sparn. The program is taught by the professors, but guided and nurtured by the love of Esther. Thank you so much.

CONTENTS

CHAPTER

1. INTRODUCTION	1
2. MAJOR SOURCES IN PACKET TECHNOLOGY	6
ALOHA	7
ARPANET	11
Other	21
3. TECHNOLOGICAL CONSIDERATIONS	26
Computer Communications	27
Microprocessors	32
Advantages and Disadvantages of Packet Radio	36
Attributes for a Practical Packet Radio Network	42
Frequency Band	42
Coexistence	44
Transparency	46
Tactical Operations Versus Mobility	46
Rapid and Convenient Deployment	48
Unattended Operation and Reliability	50
Area Coverage and Connectivity	51
Traffic Handling and Error-Free Performance	52
Other	53

CHAPTER

4. PROTOCOL CONSIDERATIONS	57
Applications	64
Untangling the Maze	68
Internal Network Protocols	71
Network-Access Protocols	71
Process-to-Process Protocols	73
Application-Oriented Protocols	73
Internetworking Protocols	74
Levels of Interconnection	77
Datagram Versus Virtual Circuit Service	80
Routing	87
Multiaccess Protocols	97
Spread Spectrum Multiple Access (SSMA)....	100
Carrier Sense Multiple Access (CSMA)	104
5. THE EXPERIMENTAL PACKET RADIO	113
The Packet Radio Unit	119
Network Management and Operation	129
Packet Radio Repeaters	129
Conclusion	132
6. MILITARY APPLICATIONS OF PACKET RADIO	134
7. CONCLUSION	144
BIBLIOGRAPHY.....	148

FIGURES

Figure

2-1	Original ALOHA System.....	8
2-2	ALOHA System UHF Radio Communications System..	9
2-3	Devices Interconnected in ALOHA, 1974.....	12
2-4	Evolutionary Growth of the ARPANET.....	14
2-5	ARPANET Configuration in September 1979.....	15
2-6	ARPANET Geographic Map, December 1980.....	17
2-7	ARPANET Logical Map, December 1980.....	18
2-8	DDN Schedule.....	20
2-9	Planned Operation of a DTS Network.....	23
3-1	Packet Radio Network.....	28
4-1	ISO Open System Interconnection Reference Model.....	59
4-2	ARPANET Protocol Layering.....	62
4-3	Approximate Correspondences Between the Various Networks.....	65
4-4	Possible Protocol Architecture Layout for Future DOD ARPANET Usage.....	67
4-5	Relationship Between Network Protocols.....	70
4-6	Basic Catenet Model.....	76
4-7	Pup Encapsulation in Various Networks.....	85
4-8	Use of a Hop Counter for Flooded Routing.....	90
4-9	Point-to-Point and Broadcast Routing.....	92
4-10	A Repeater Tree Labeling.....	94

Figure

5-1	Location of Major Elements of the Packet Radio Tested During 1977.....	115
5-2	Experimental Packet Radio Configuration.....	120
5-3	Upgraded Packet Radio Configuration.....	125
5-4	UPR Digital Section Architecture.....	128

CHAPTER 1

INTRODUCTION

Radio propagation plays a major role in the telecommunications field commercially and militarily as a source of transmission media. In recent years the issues based on scarcity in available spectrum evolved to new forms of frequency reuse schemes and more efficient utilization of the spectrum. The military considers it vital to appropriate this technology for radio transmission. The fluid capability of establishing radio communications still outweighs any other source for rapid deployment. Terrestrial packet radio enhances this capability by taking advantage of radio transmission mobility and the interoperability it allows between integrated data systems.

A packet radio network permits a protraction from other telecommunications systems. All the functions of the original packet system (switching, transmission, coding, etc.) may stand alone and be unaffected by a packet broadcasting network. For this reason current trends in packet switching represent a vital link for the technological growth of packet broadcasting

networks. In response this study focuses first on sources appearing in packet technology which may act as the backbone system for adhoc, packet, radio, communication networks.

Packet radio represents a growing transmission media for data communications between computer hosts, remote terminals, teletypes, video displays and much more. Most of the current research and development is engaged in applying the technique to military communications because of the mobility of its applications. The issue of interoperability, or how to make different parts of military communications compatible across service lines (or even intraservice lines), stimulates a large part of the research. Networking between strategic communications, tactical communications or both profits from a data transmission media which enhances the command and control options of military leaders.

Three technical developments in the early 1970s prevail as breakthroughs that permitted the evolution to a practical packet radio network. The growth of microprocessors, and the memory technology which expanded at incredible rates along with the microprocessor, implementation of surface acoustical wave (SAW) technology, and innovation of protocol techniques between computer and communications communities are the pillars around which the whole technical efficiency of packet radio revolves.¹ From these developments the possibility of operational

packet radio networks through hand held terminals, as small as the Hewlett-Packard's HP-65 pocket computer, became possible.² With this implied dramatic change in transmission media there is a responsibility for thorough evaluation by the military services for its integration into the Defense Communications System (DCS).

An examination of the technical advantages and disadvantages of packet radio as well as purely military considerations is required. As a communication (transmission) technique for military purposes, specifications far beyond those of a practical commercial system must be considered. The wartime environment criteria places special emphasis on security, terrain, survivability, redundancy, durability and mobility, just to name some of the major considerations. In every situation the threat evaluation dictates the design characteristics for each piece of equipment and software supporting the network, and the operational parameters within which each must operate.

This study approaches the purely military applications of packet radio even though the technology can be used commercially. With the advent of cellular radio, after many years of consideration by the Federal Communications Commission, a packet system could be used as an alternative or a complement. This area provides many avenues of exploratory research still to be tried for commercial applications.

A recommended program will be examined for a military packet radio network. The Advanced Research Project Agency's (ARPA) creation of the ARPANET has the closest approach to creating a military network yet proposed. Though still in research stage, considerations for the implementation of packet radio started in their experimental packet radio network, PRNET.³

NOTES, CHAPTER 1

¹ Robert E. Kahn, Steven A. Gronemeyer, Jerry Burchfiel and Ronald C. Kunzelman, "Advances in Packet Radio Technology," Proceedings of the IEEE, November 1978, p. 1469.

² James Martin, Future Developments in Telecommunications, Prentice-Hall, Inc., 1977, p. 385.

³ Kahn et al., p. 1469.

CHAPTER 2

MAJOR SOURCES IN PACKET TECHNOLOGY

The most important source in packet radio technology research originates from the Department of Defense Advanced Research Project Agency (DARPA). As the sponsor for the ALOHA system and the creator of the ARPANET (1968), DARPA provided the theory which is driving today's technology toward a practical terrestrial packet radio network.* A transition which occurred in the mid-1970s advanced the cause of packet technology from experimental to operational.¹ This transition took place as a direct result of DARPA research, and is the basis through which packet radio could easily become a wide source of transmission. This research applied to terrestrial wire, terrestrial radio or satellite channels also demonstrates its value for communications either for a local or a large area distribution of data.

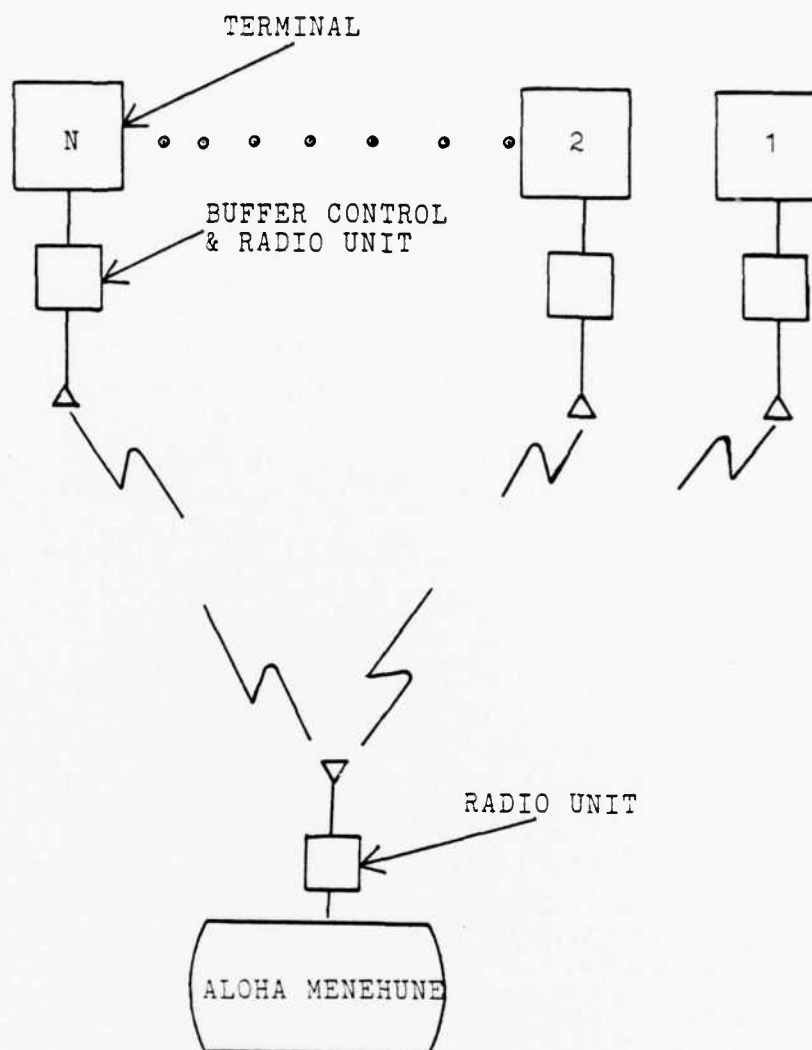
The Department of Defense Advanced Research Projects Agency (DARPA) made it possible to go beyond packet switching. As a smaller element of the whole

*Note: From this point on terrestrial packet radio will be identified as simply packet radio unless it is necessary to distinguish it from satellite packet radio applications.

system, terrestrial packet radio transmission permits new networking schemes. A multiple access radio channel becomes a highly efficient medium supporting large numbers of potential mobile subscribers of packeted information.² Through the use of specific interface units a mobile/tactical network of packet radios can fit easily into the protocol architecture of defense communications. The possibilities for usefulness are staggering when considered as an element of military field forces.

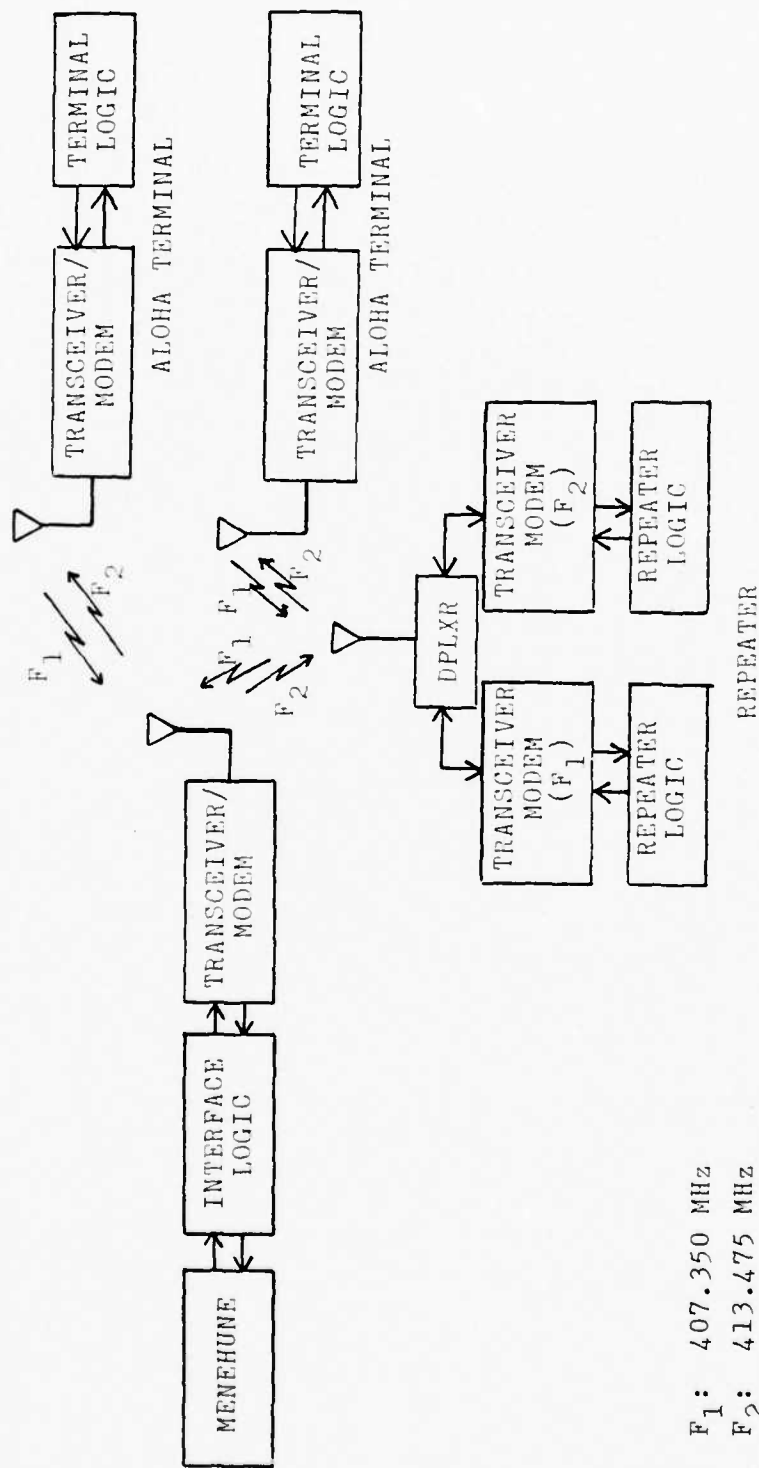
ALOHA

The Additive Link On-line Hawaiian Access system, ALOHA, was supported by DARPA as a research project at the University of Hawaii. It illustrates the earliest example of an experimental packet radio network. Figure 2-1 is a system overview of the original ALOHA network. ALOHA provided access to the Menehune (Hawaiian for IMP) computer in Honolulu from different locations on the Hawaiian Islands.³ The terminals communicating to the host computer transmitted data through a terrestrial UHF (Ultra-high frequency) radio using two different frequencies; one for transmitting and one for receiving. Figure 2-2 represents the resultant configuration of the ALOHA UHF radio communication system. Combining the features of packet switching with broadcast channels for a data communication network demonstrated



Source: Robert E. Kahn, "The Organization of Computer Resources into a Packet Radio Network," IEEE Transactions on Communications, vol. COM-25, no. 1, January 1977, p. 170.

Figure 2-1 Original ALOHA System



F₁: 407.350 MHz
F₂: 413.475 MHz

Source: R. Binder, N. Abramson, F. Kuo, A. Okinaka and D. Wax, "ALOHA Packet Broadcasting-A Retrospect," AFIPS Conference Proceedings, Anaheim, 1975.

Figure 2-2 ALOHA System UHF Radio Communication System

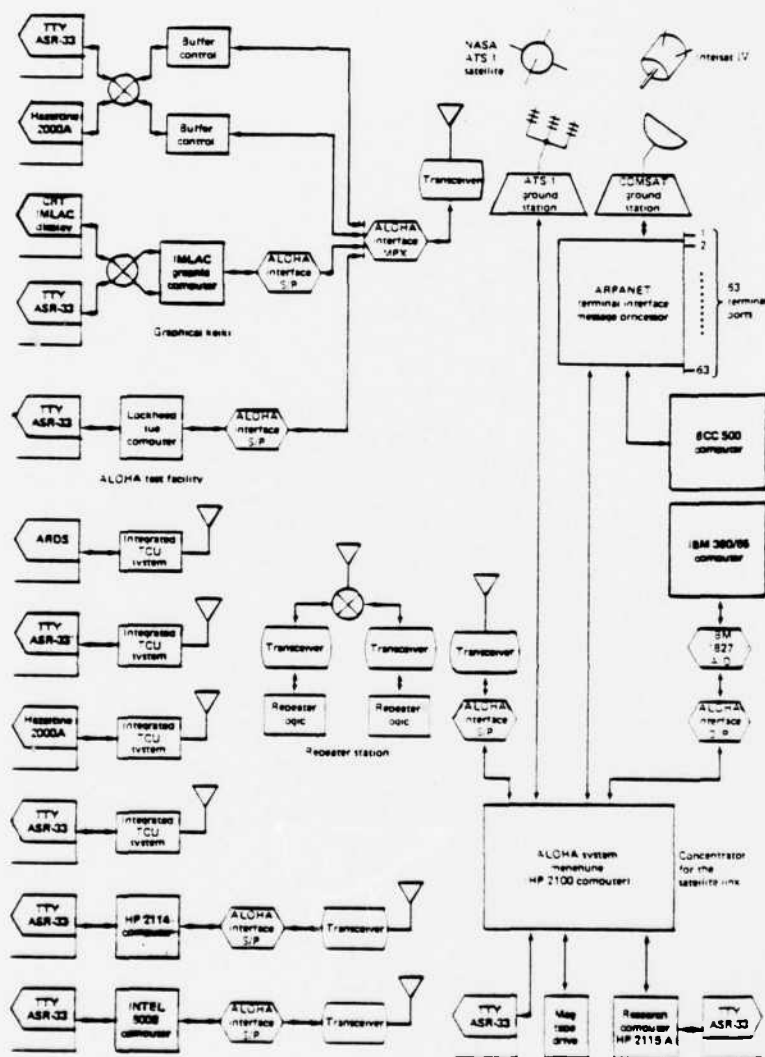
a revolutionary design in distributed packet networks using a contention protocol.⁴ The data transmitted between terminal and host computer resembled fixed length packets of information preceded by a header and appended with a checksum. The theory for this system acknowledged that retransmissions were a basic element of channel utilization, since contention protocol by its very meaning indicates that some transmissions will not be successful. This suggests an independence of the transmitting terminal in the network to its interaction with the host computer. This is the essence of the ALOHA system and implies a very important property both detrimental and vital to a packet radio network. The ALOHA system made a significant contribution to the advancement of radio-linked computer networks. ALOHANET still furnishes a real-time experimental design that drives current satellite protocol considerations.

ALOHANET of the ALOHA system, embodies meanings beyond the original system designed at the University of Hawaii. ALOHA stands alone as a designation of much broader interpretations and values. In the Hawaiian language ALOHA is used as a personal greeting for arrival and departure. In communications, ALOHA specifically relates a protocol technique (contention) which predicts arrivals and departures of packetized data.⁵ ALOHA or the ALOHA channel represents a conceptual model of a distributed network of terminals vying for the attention of a host

computer. The network originally devised at the University of Hawaii applied the techniques of ALOHA with terrestrial broadcast radios. This technique closely defines variables necessary to a terrestrial packet radio network. In much of today's literature ALOHA technique is applied to satellite protocol systems, since they contain the same types of broadcast considerations (except for delay times). Figure 2-3 illustrates the flexibility of the ALOHANET for adding different types of devices to the network. ALOHA also implies fixed channel utilization values (maximum). Empirically, simple ALOHA represents a maximum useful channel throughput of $1/2e$ or 18.4 percent, while a variation called slotted ALOHA doubles the capacity to $1/e$ or about 37 percent.⁶ The important conclusion to draw is that ALOHA defines the basic "no cooperation" protocol with a universal meaning and with values that represent the same thing to many people.⁷ This therefore allows "ALOHA" to be used as a word without applying the original acronym.

ARPANET

The ARPANET, like the ALOHANET, employed packet switching in a computer network of distributed nodes. Unlike ALOHANET, ARPANET was not designed as a broadcasting network but operates as a guided wave system. In 1969 the network unfolded with four nodes on the west



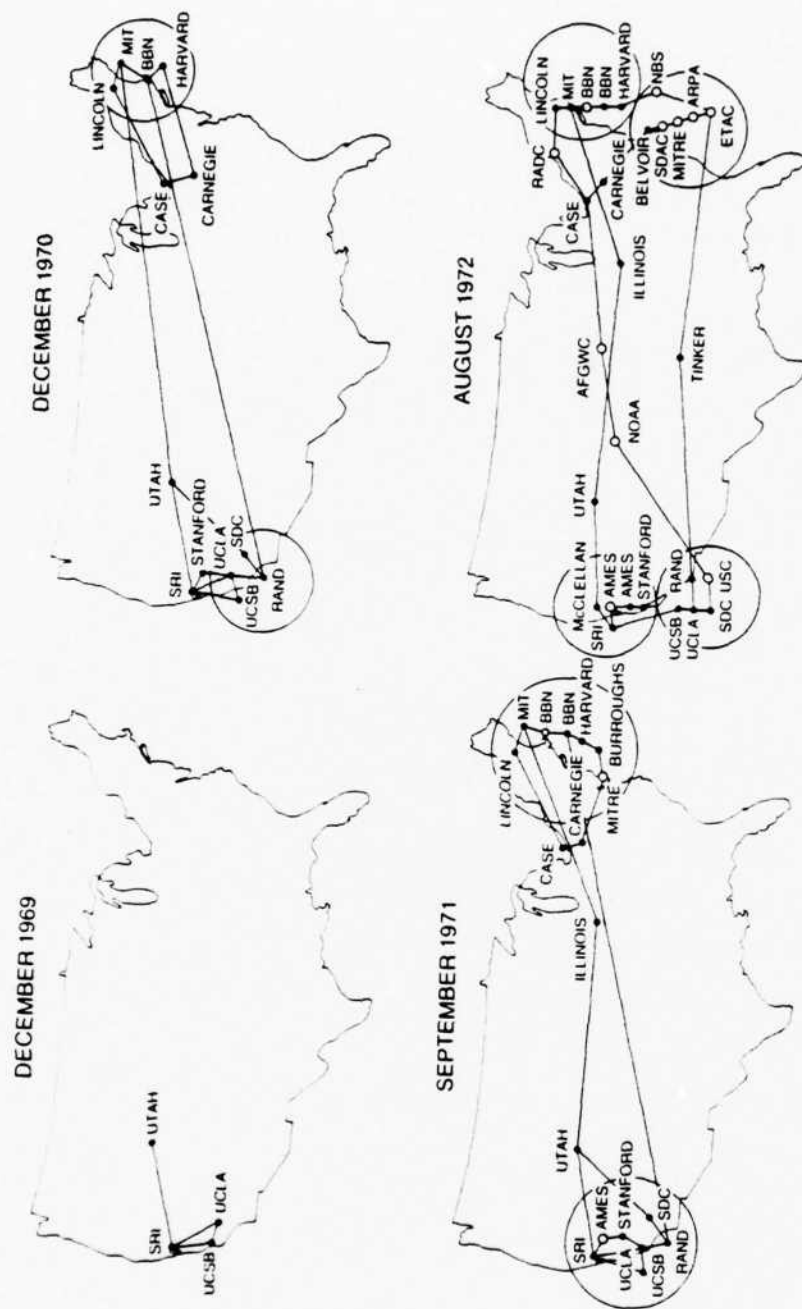
Source: James Martin, Communications Satellite Systems, Prentice-Hall, Inc., 1978, p. 324.

Figure 2-3 Devices Interconnected in ALOHA, 1974

coast of the United States. A year later the network expanded from coast to coast, and by 1979 it grew to sixty-four nodes with satellite links to England, Norway and Hawaii. Figures 2-4 and 2-5 show the evolution of the ARPANET from 1969 to 1979. ARPANET is the best known packet-switching network and a foundation of principles for commercial expansion of this technology.⁸

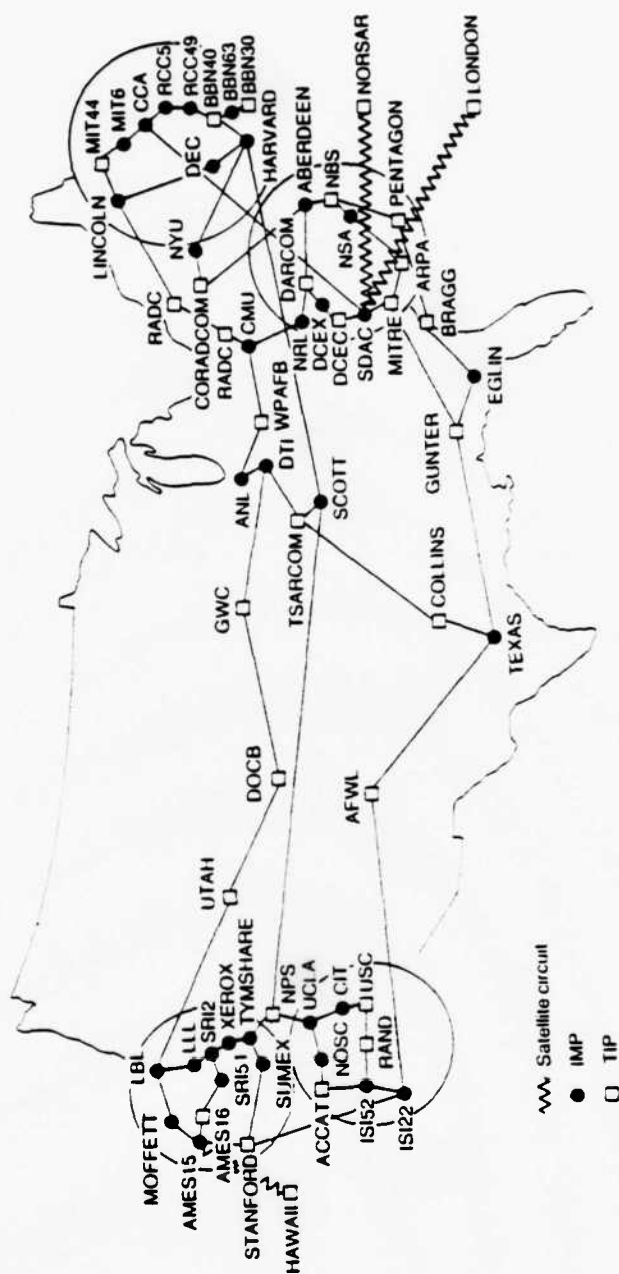
Configuration of the ARPANET consists of three main types of physical nodes. The interface message processors (IMPs) are the first type. They serve two functions: they act as the interface to host computers, or a store-and-forward switch for the independently routed (virtual circuit) packets in the network. The second type is the terminal interface message processor (TIP) which executes an additional function above the IMPs. The TIPs provide access to the network for unintelligent terminals by accomplishing the additional concentrator function of packets. And the last type is the network control center (NCC), which is added to the operating system for network monitoring, diagnostics and maintenance. The NCCs are vital to the operating system since they add the control for host-to-host protocol and a multiplexing function for multiple hosts.⁹

ARPANET, a single user network, is considered as a private "public" network since it serves a limited community (commercial research and development, universities, Department of Defense, government agencies, etc.)



Source: Roy D. Rosner, Packet Switching, Lifetime Learning Publications, 1982, p. 167.

Figure 2-4 Evolutionary Growth of the ARPANET

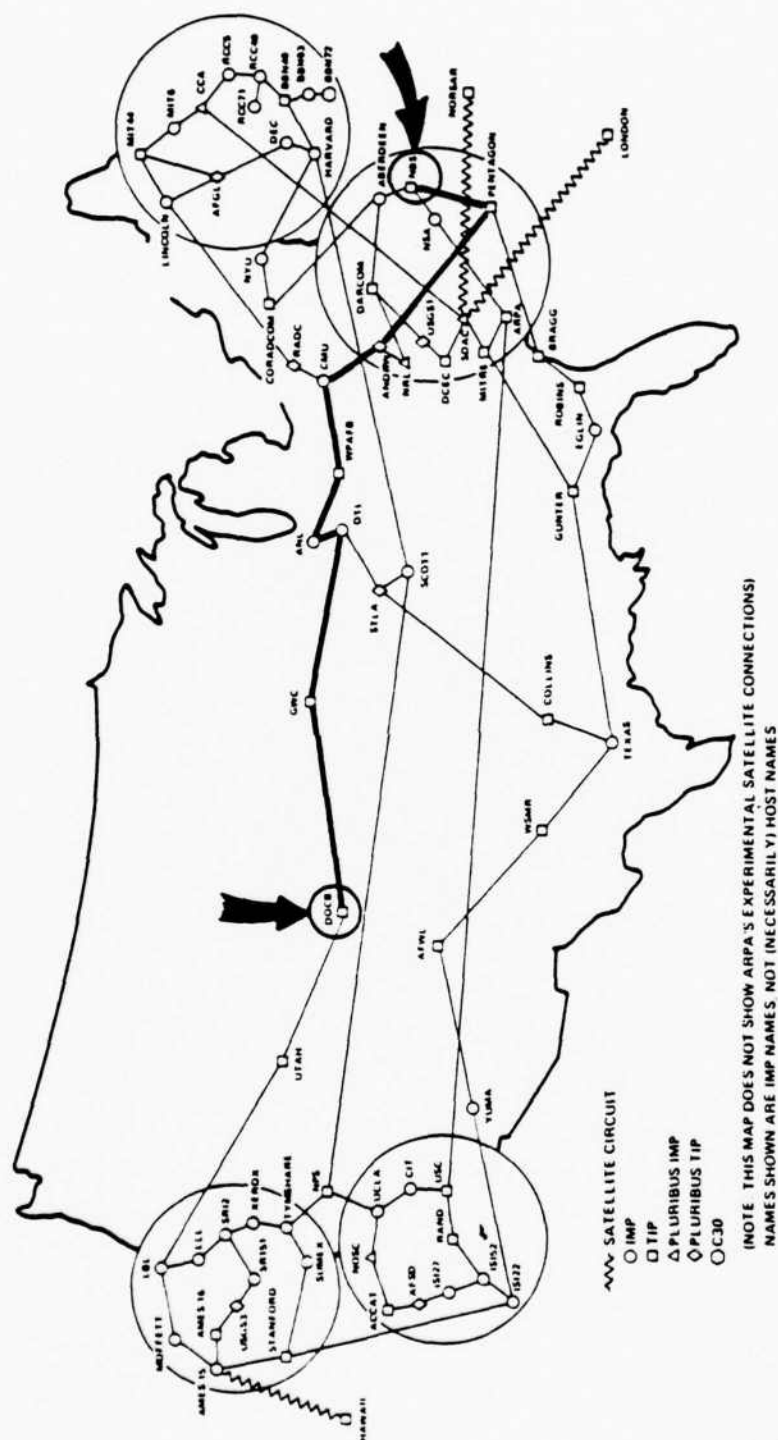


Source: Roy D. Rosner, Packet Switching, Lifetime Learning Publications, 1982, p. 170.

Figure 2-5 ARPANET Configuration in September 1979

and allows equal access from any node.¹⁰ Figure 2-6 shows a topological view of the subnetwork in December 1980 with the Department of Commerce, Boulder (DOCB) and National Bureau of Standards (NBS) TIPS highlighted. A logical representation of the ARPANET is provided in Figure 2-7 showing the connected host computers. The details of ARPANET show up in almost every technical journal and therefore provide the private sector with valuable information on the technology without cost. Although conceived as a nonbroadcast network, ARPANET's expansion into broadcast applications demonstrates flexibility and originality of design. Like ALOHANET, ARPANET supplied the first generation application of packet switching techniques and an operational model for commercial application. Contributors to the ARPANET list as a WHO's WHO in major communication and computer technology. This outstanding application of technical progress acts both as a model for operational systems and as a stimulant for continued progress.

Composed of multiple nodes the ARPANET reaches both government (federal) and non-government entities. In defining the ARPANET, a basic system used for theoretical premises in packet technology, one must view it as a system that can be partitioned into two distinct components. The non-government entities consist of private companies such as Mitre, Rand, Xerox, Collins and Tymshare, and major universities around the country to



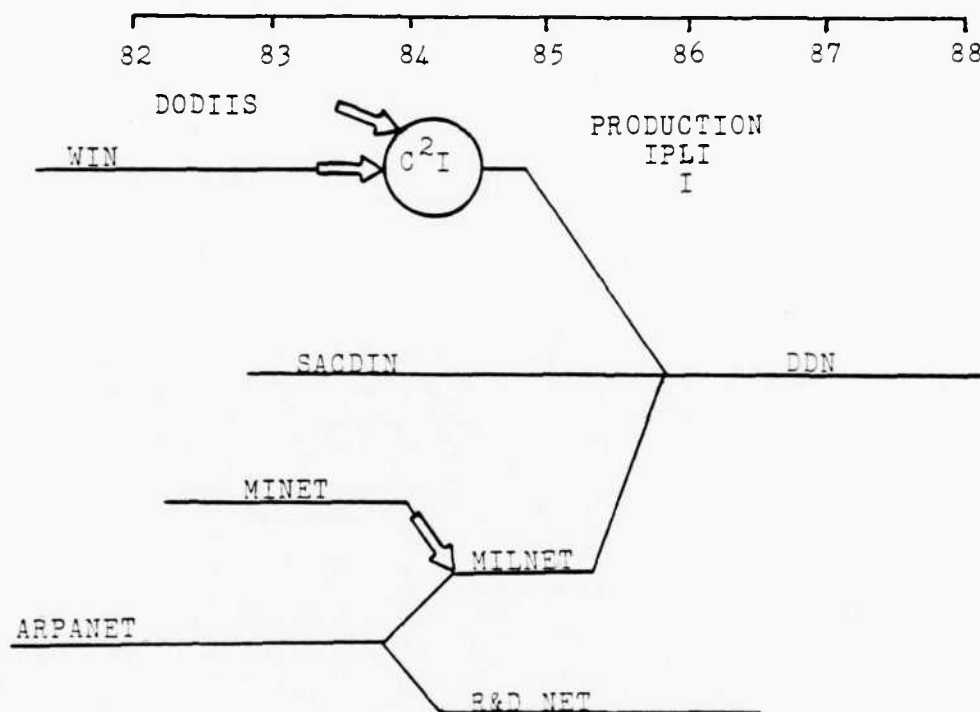
Source: NTIA Report 82-112, November 1982, p. 9.

Figure 2-6 ARPANET Geographic Map, December 1980

include Harvard, Rutgers, Stanford, UCLA, Hawaii and MIT. This part of ARPANET can be distinguished as the research and development segment. A major part of the network belongs to the Department of Defense (DOD) and extends to the Pentagon, and Army, Navy and Air Force installations. A military packet radio system applied to the DOD portion of the network would provide an interface into the Defense Communications System (DCS) by tactical operations. It is important to note that the non-government entities of this network technically represent a valuable research asset to the government use of packet technology. For this study, we will direct the subject matter to the DOD components in the network.

The DOD components of ARPANET face a near-term reorganization into a contracted military network called MILNET, an acronym for military network. The eventual outcome of MILNET will be an interoperable, multi-level, secure network called the Defense Data Network (DDN). The DDN, based on ARPANET technology, satisfies requirements of the Defense Department for an intercomputer telecommunications network. This data network takes on the role of command, control and communications with worldwide wartime survivability.

The initial steps taken for the DDN began in 1982. The schedule for implementation of the DDN can be seen in Figure 2-8. Three working military networks ARPANET, WIN (WWMCCS Intercomputer Network) and MINET



Source: Heidi B. Heiden, "Defense Data Network,"
Fifteenth Annual Electronics and Aerospace
Systems Conference, Washington, D.C., September
 20-22, 1982.

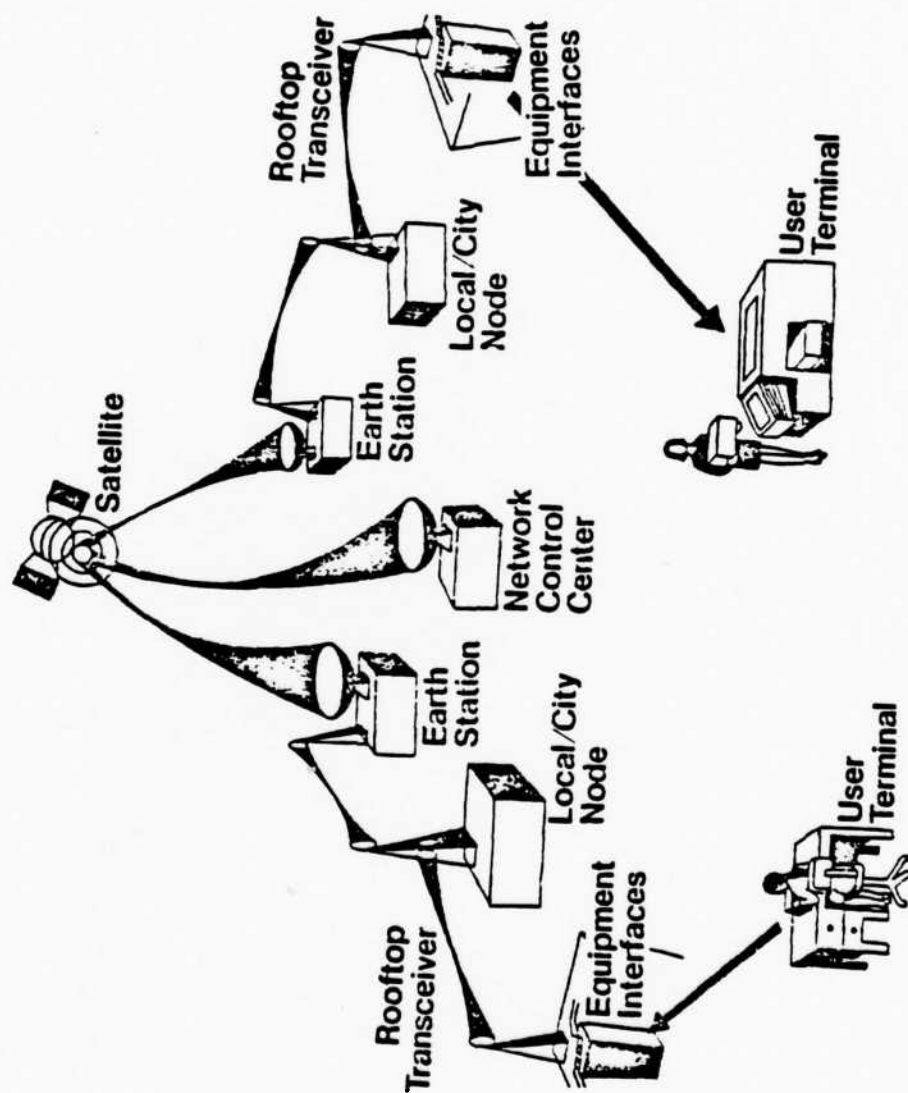
Figure 2-8 DDN Schedule

comprise the network which will be the backbone for the DDN, with the addition of SACDIN (Strategic Air Command Digital Network) which is still in various stages of development. The final product will yield a highly survivable network with a dense grid of backbone trunks using dynamically adaptive routing. All nodes will be at military sites for physical security and use both end-to-end and link encryption for transmission security.¹¹ Since standardization of protocols will be employed, to include interface protocols, the possibilities of connecting asynchronous and synchronous terminals from a packet radio network to DDN exists as a viable option.

Other

Nationwide in the United States three major commercial packet switching systems supply value-added, switched, service networks. General Telephone and Electronics Corporation's (GT&T) Telenet (Communications Corporation) was the first commercial packet switcher. Since then Tymnet Incorporated and Graphnet Communications expanded the competition nationwide as well as to non-U.S. networks.¹² As sources of packet technology and more importantly gateways for adhoc packet radio networks, the expansion of the digital transmission medium becomes a more relevant extension beyond the purely military applications.

The Digital Termination System (DTS), used commercially to bypass the congestion of the local loop, contains a broadcast strategy for local distribution requirements. With the surge in large city teleports the need for efficient distribution of satellite downlinks (and uplinks) has become more pressing. RAPAC or Radio Packet Communications System, the radio based DTS, employs packet radio techniques in cellular-form for distribution of digital information.¹³ Figure 2-9 represents a proposed RAPAC based DTS system that was submitted by the Xerox Corporation. A central broadcasting site, in an allocated frequency band of 10.55 to 10.68 GHz, is used specifically for high-speed digital data traffic.¹⁴ A typical system configured into cellular-form sends packeted data to users in large metropolitan areas. Users may include individual companies, or one or many of the value-added, packet switched, service networks. The RAPAC form of DTS (also Cable Packet Communications System, CAPAC) is a packet radio strategy which uses microwave antennas with beamwidths of up to 120 degrees, so that it may reach many users in a given cell. Originally a Xerox Corporation creation in 1978 called XTEN (See Figure 2-9), the DTS proposal has since been presented by as many as thirty-two possible applicants before the Federal Communications Commission.¹⁵ The consensus in industry is that DTS is a stop-gap measure for the local loop congestion problem until



Source: Xerox Petition for Rulemaking, 1978, p. 6.
Figure 2-9 Planned Operation of a DTS Network

sufficient fiber optics become available. The significance of RAPAC to packet radio is the fact that operationally it is successful, and cost-wise it is not expensive to implement. Lessons may be learned from the DTS experience and improve the chances for packet radio technology.

Packet radio distends the application of packet switching to broadcasting, which requires different considerations. Satellite access methods resemble those of purely terrestrial packet radio except for the longer delays involved with a geosynchronous repeater, such as is the case with a satellite. ALOHANET has been a very influential tool in the study of satellite packet radio systems and typifies some of the features in terrestrial packet radio. Although each of the comparisons (ALOHA-NET, ARPANET, commercial packet switchers, DTS and satellite packet radio) differ in some respects to terrestrial packet radio, they all support a total system in which each is a part. For military applications the possibilities of gateways from one system to the next represents a quantum leap toward the goal of interoperability. More importantly digital communications represent the wave of the future, especially concerning communications for distributed information systems. Packet radio characterizes the link that is possible from tactical and mobile operations into the backbone of the Defense Communications System.

NOTES, CHAPTER 2

¹ Norman Abramson, "The Throughput of Packet Broadcasting Channels," IEEE Transactions on Communications, January 1977, p. 117.

² Leonard Kleinrock, "Principles and Lessons in Packet Communications," Proceedings of the IEEE, November 1978, p. 1320.

³ R. Binder, W.S. Lai and M. Wilson, "The ALOHANET Menehune-Version II," ALOHA System Technical Report B 74-6, University of Hawaii, September 1974.

⁴ Abramson, p. 117.

⁵ Roy D. Rosner, Packet Switching, Lifetime Learning Publications, 1982, p. 214.

⁶ Ibid., pp. 223-236.

⁷ W.R. Franta and Imrich Chlamtac, Local Networks, Lexington Books, 1981, p. 57.

⁸ Wushow Chcu, ed., Computer Communications Volume I Principles, Prentice-Hall, Inc., 1983, p. 9.

⁹ Ibid., p. 68.

¹⁰ Ibid., p. 68.

¹¹ Heidi B. Heiden, "Defense Data Network," Fifteenth Annual Electronics and Aerospace Systems Conference, Washington D.C., 1982, p. 75.

¹² Rosner, p. 277.

¹³ Ronald A. Frank, "Beyond Local Loops," Datamation, vol. 28, no. 4, April 1982, p. 93.

¹⁴ Richard V. Palermo, "Data in the Fast Lane: Digital Termination System," Satellite Communications, March 1983, p. 22.

¹⁵ John Tysko, "New Transmission Media for Local Loop to Reshape Telecommunications," Data Management, vol. 20, no. 4, April 1982, pp. 24-25.

CHAPTER 3

TECHNOLOGICAL CONSIDERATIONS

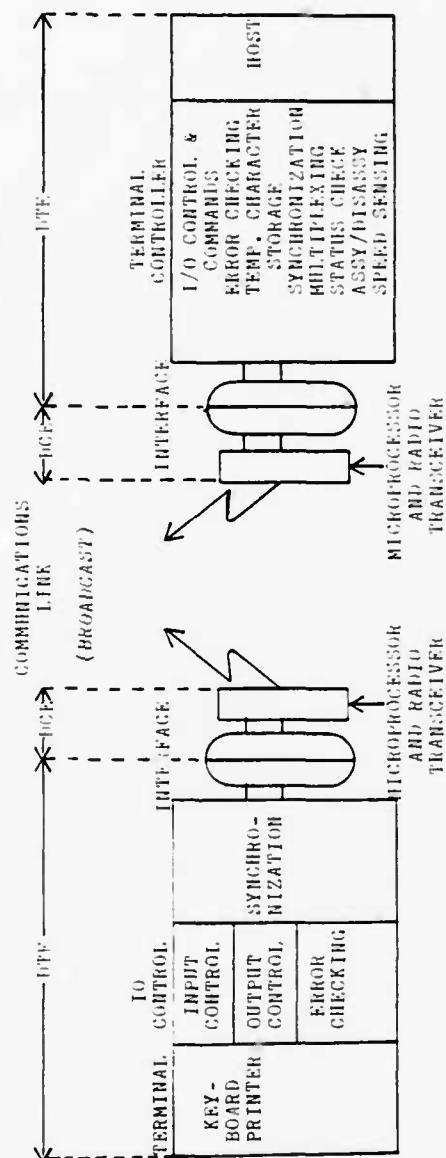
The possibility of discussing every technical consideration thoroughly for a packet radio network is beyond the scope of this study. What is attempted is an overview of major considerations which would affect a network that would serve a military purpose.

Since the federal government, and particularly the Department of Defense (DOD), is one of the major developers of computer networks,¹ the first section of this chapter includes those considerations for a military computer network. The use of packet radio provides an economic solution² to the defense department's information transfer requirements among mobile users and computer resource sharing. With the growing demand for data services, implementations of more effective computer communications technology has become a necessity for the command and control (C²) of the vast amounts of resources in the DOD. Computer systems which interact within the Continental United States (CONUS) as well as to locations across oceans and international borders require a special emphasis in communications technology. The technological success of providing the transmission

media as well as the myriad requirements for error-free transfers depends logically on interfacing the computer network with various forms of communication techniques. With this in mind, packet radio used as one technique of connecting a distributed local computer network meets this growing need in the DOD, and therefore must be considered a valuable asset for implementation.

Computer Communications

The basic model from Figure 3-1 for a computer communications network contains first the element called data terminal equipment (DTE).³ The DTE includes a data source, a data sink or both.⁴ Sources are comprised of the equipment that supply the data that will be transmitted. They include such devices as the computer, the data terminal, video equipment or digital facsimile. Each consists of digital functional units emitting data streams. The data sink is that equipment which checks the data and originates error-and system-control signals. The data communication system-control is performed in accordance with the various protocol levels.⁵ The equipment used in the DTE may be a single item, which provides all the required functions, or multiple end-items of equipment interconnected as a subsystem. This is an important consideration for military applications since the multiple pieces of equipment may include communications security equipment (for encryption).



Source: Adapted by thesis author

Figure 3-1 Packet Radio Network

While the DTE is the end of the data link, the next component, the data circuit-terminating equipment (DCE) is the end of the line, before being put on the communication link (channel). The DCE begins at the end of the data circuit and acts as the interface equipment into the channel. Usually installed on the user's premises it provides all the functions that establish, maintain and terminate a connection. Classified sometimes as the network terminating unit, the DCE provides coding and signal conversion between the DTE and the channel. As was the case with the DTE, the DCE may be a single piece of equipment; yet it may also be an integral part of another unit, such as the DTE.⁶ This section may also contain additional communications security devices.

The final medium before re-entering another DCE-DTE model is the communication link or channel itself. For packet radio this consists of the broadcast medium of free space. An antenna converts the electrical energy from the transmitter into electromagnetic waves. This act of transforming energy from one form to another is called transducing. Currents from the antenna launch the final information units into waves that represent, in some manipulated form, the original information. Hence on the receiving side the antenna retransforms the electromagnetic waves into energy that can be re-evaluated through the receiver unit into the

DCE-DTE model.⁷ In the military environment this broadcast medium represents two obstacles: the lack of available spectrum and the alterations of electromagnetic waves that destroy the information contents. These two obstacles will be more precisely defined later in this chapter.

The meaning of the term computer communication can be further classified into three categories:

Interpretation (1)

An interconnected group of independent computer systems which communicate with one another and share resources, such as programs, data, hardware, or software. With this definition, computers used solely for handling communications or controlling terminals are excluded.

Interpretation (2)

An interconnected group of independent computers and data terminals which communicate with one another. With this definition, computers used for handling communications or controlling terminals, such as concentrators and terminal control units, are included.

Interpretation (3)

Any data communication network which consists of at least one computer system. With this definition, there is almost no distinction between data communication and computer communication.⁸

For this discussion the data communication definition (3) will be excluded entirely, since it usually means terminal-oriented networks where no computer-to-computer communication takes place.⁹ We also stipulate that the communications function involves packet technology. Data generated through the DTE will be finalized for

transmission in individual packets of information. The form of these packets will generally be a fixed length. Packet switching technology will be the means to route the packets in the broadcast medium to a final destination.

Interpretation (2) most resembles a military application for mobile data terminals. In many cases computer-to-computer systems as defined in (1) dictate an extremely stringent error-free environment. Although not eliminated, packet radio technology still has difficulty supporting Interpretation (1) as well as it will support Interpretation (2). A major system with one main computer which reaches distributed terminals as in ALOHANET is the easiest to support by the broadcast medium. Note that in ALOHANET the terminals were fixed. A similarly applied military network may include terminals that must communicate on the move. The movement by prospective terminals further complicates the ability for two high-speed computers to communicate. A low-speed terminal on the other hand is not as complex, and can be one of many terminals communicating to a main computer whose capabilities far exceed those of a single terminal. We are also interested in Interpretation (2) because the tactical terminals in a military field maneuver will be in contention for computer time. Therefore the terminal control will be a vital consideration each time the network reconfigures.

Microprocessors

A key technological consideration for building a packet radio network is the state of the art in current microprocessors. Basically a device which executes simple instructions, the microprocessor technology is growing by leaps and bounds to include much more sophisticated processing. Microscopic circuitry, with current advances in large scale integrated chips, can produce computer capabilities in simple hand held devices. A separate but complementary technology, memory capabilities, exceeds even the growth of the microprocessor technology. Between the two, computers small enough to carry in your pocket are being produced that have as much power as a second generation IBM processor (like the 1401). Requiring no air-conditioning or large power supplies, the same small pocket computer has four times the memory of the larger second generation IBM computer.¹⁰ Amazing results should continue to occur with the recent advances in very high-speed integrated circuits.

The microprocessor used in a packet radio must handle the logical functions of packet processing. It must control access to the common radio channel and dynamically do scheduling to minimize or avoid conflicts. As a supervisor using an executive program, the microprocessor must exercise terminal control. The terminal,

operating in a multiprogrammed environment, will be reacting to network reconfigurations and fluctuations under real-time demands. The store-and-forward function of the network can be easily managed in the microprocessor as well as managing network changes. Processing times will be very important to the packet radio network. A basic network must achieve a rate of 100 kilo bits per second (but even slow microprocessors can handle rates in excess of 100 Kbps).¹¹ The terminal may be configured using separate microprocessors for the keyboard and the display control, and for the radio processing. The design stage must consider the partitions that might be necessary in order to operate on-line and off-line.

The requirements of the microprocessor increase for repeaters and become even more complicated when used at stations. The following is a list of desired communication capabilities for each of the network devices. Each must be considered within the software applications for the microprocessor:

Terminals: Requirements include:

1. Ability to identify packets addressed to it.
2. Calculation of packet checksum.
3. Capabilities related to packet routing such as; retransmitting packets when acknowledgments are not received, recording and using a specific ID of a repeater and/or station to be used for other packets of the same message, counting the number of retransmissions.

4. Capabilities related to the response to previously determined types of error.
5. For unattended terminals, capabilities by which a centralized control or a station will be able to identify whether the terminal is operative or dead.

Repeaters: Requirements include:

1. Calculating packet checksum.
2. Packet storage and retransmission.
3. Capabilities by which a station can determine whether a particular repeater (or any repeater in a particular area) is operative or dead.
4. Capabilities 1, 3, and 4 of terminals.
5. Capabilities, dependent on the routing strategy, for calculating the most efficient next repeater on a transmission path to a station or to a terminal.

Stations: Requirements include:

1. A dynamic directory of active terminals and repeaters in its region.
2. Gateway functions necessary to transfer packets between the Packet Radio System and another network.
3. Storage buffers for packets received from terminals and for packets to be transmitted to terminals.
4. Storage for character position information for active terminals which do not have this capability.
5. Accounting capabilities.
6. Capabilities related to routing, flow control, and network management.¹²

For a military network, repeaters and terminals might be a combined element. It may not always be feasible to deploy a backbone network, due to the environment. Therefore a user's radio may have to "double up" as a repeater to support other traffic.¹³ This has significant implications toward microprocessor capabilities.

In addition to those functions in the terminal itself, some provisions must be made to include capabilities for imitating a repeater at each terminal.

Another consideration must be included for physical layout of encryption devices with the microprocessors. At the terminal position, a microprocessor on either side of the encryption device supports the keyboard display on one end, and as a part of the packet radio, provides the logical functions independent of the encryption process. Each is handled separately by the microprocessor and assumed to be encrypted independently. The repeater, accepting packets and then forwarding packets, cycles through a series of confirmations, storage and acknowledgments in order to verify each encrypted packet and route it to the next repeater. The microprocessors have multiple roles in this situation, demanding more vigorous requirements of the microprocessing sections.¹⁴

The microprocessor technology has moved from hardwired terminal control units (TCU) to fully programmable control units (PCU). Greater reduction in size of chips, increased processing power and speed, and reduced external interfacing hardware has advanced the flexibility of microprocessors.¹⁵ In these respects, the cause of packet radio networks is also advanced as older problems of size, power and complexity are overcome by the new microprocessor technology.

Advantages and Disadvantages
of Packet Radio

A review of advantages and disadvantages is necessary in order to consider the technological consequences of providing packet radio technology. Major interests of concern to a designer are the limitations, and the characteristics which are favorable for his design. The following discussion will cover these considerations.

Packet radio extends the applications of packet switching while utilizing packet switching communication techniques. As an extension of this digital network, packet radio answers the demands in computer communications and the need for network resource sharing, and between the two, offers a cost effective means of distributing data communications. A comparison of cost trends in packet switching showed that cost trends in communications were falling due to the advances in state of the art electronics. Where possible, switching has replaced transmission because of its relative cost advantage over the more regulated transmission environment. On the same scale, computing trends have out-distanced communications in falling prices. For example, in 1969 the cost of communications and computing were approximately equal at \$.5/million bits of data. Six years later, 1975, the cost of communications had fallen by

half to \$.25/million bits, while computing had fallen to approximately \$.038/million bits, less than one-tenth of its value in 1969. The composite packet switching costs for this same period fell from \$.9/million bits to \$.3/million bits of data. Comparing costs for packet switching techniques and computer communications distribution revealed three major cost components: processing, large-capacity nationwide transmission, and local or regional communications to the nearest point where economics of scale were possible. This comparison introduces the element of low-cost high-capacity carriers. The results indicated that local connection costs, while cheaper than land-line costs, were much higher than the costs of computing, or the cost of transmission through the long-distance high-capacity carriers. Packet radio techniques offer a new way to reduce the local costs while utilizing the falling cost trends in packet switching. This offers a unique opportunity for military applications by providing a means to share automation without the cost of dedicated lines or without the restriction for economies of scale.¹⁶

The broadcast medium used by packet radio offers some distinct advantages. As a method which offers a highly efficient way of utilizing a multiple access radio channel, packet radio provides efficient spectrum utilization. In the broadcast domain it can support many users, who are mobile, over a wide geo-

graphic area by applying omnidirectional techniques. This not only supports mobility, but also offers advantages in the military tactical environment. In an area where there are no phones or backbone communications capabilities, packet radio takes advantage of its abilities to meet communication demands without having to provide extensive engineering. This works well in areas where the elements of nature are hostile, such as deserts and swamps. Within the broadcast domain packet radio also offers the possibility of coexisting with other systems through the use of coded multiple access techniques, like spread spectrum. Broadcasting too is one of the oldest forms of communications, so familiarity with its characteristics permits a designer to compensate for disadvantages.

Packet radio communications can be defined as: a digital radio application with "bursty" transmissions where there is a very low duty cycle and only short bursts of data which are sent and received. This offers all the advantages of digital technology, to include its ability to operate in noisy environments due to exact regeneration of pulses, and easy translations of data for better encryption capabilities. Because of its bursty nature enemy direction finding efforts are less effective since no continuous stream is available for lock-on. Jamming can be avoided due to the dynamic routing capabilities in the packet radio network and

the noncoherent transmission of packets. Spoofing is less effective to a network which discards invalid waveforms prior to processing, or ignores unrecognized transmissions. The overall effect is a communications network which effectively meets the threat of radio-electronic combat. Other advantages of packet radio include:

- Supports many media devices and requirements
- Flexibility and adaptability to the environment
- Allows rapid exchanges of short messages
- Permits distributed control of network management functions
- Redundancy and alternate routing capability
- Rapid deployment enhanced
- Operates in real-time
- Extension of automation to a battlefield or to crisis situations
- Provides high throughput, low delay, and a means for interconnection of networks
- Allows personal radio terminals

Probably the greatest obstacle to packet radio technology emanates from the problem of limited spectrum. While the broadcast medium offers distinct advantages for distribution over wide areas, packet radio must face stiff competition for prime frequency bands that offer low propagation characteristics which can support higher data rates. The broadcast medium is not free space as is calculated in many formulas. It must

contend with path losses, atmospheric and space effects, as well as problems of local terrain. The line-of-sight characteristics of packet radio transmission cause reflection, refraction and diffraction from hills, valleys, trees, lakes, buildings etc., which the broadcast medium amplifies in the dense atmosphere closest to the earth's surface. Many times atmospheric losses, such as those caused by rain, snow, fog, hail, etc., can not be compensated at the higher frequencies (above 10 GHz). The broadcast medium is also a political concern worldwide, and due to regulatory issues, faces obstacles that can not be overcome with technical know-how. The political (as well as natural) effects on the broadcast medium induce costs that may make new broadcast technologies, such as packet radio, unattractive. For the military, improvements through new systems must undergo extreme bureaucratic scrutiny. Private and public concerns already involved in broadcasting may pose obstacles through this process on the basis of limited spectrum, despite possible technology improvements in broadcasting. Complexity of the broadcast medium is further increased because atmospheric conditions are unpredictable. Predicting weather accurately is one problem, while predicting exactly the effects of each weather condition amplifies the complexity. Other disadvantages of packet radio include:

--Limited range

- Requirements for complex protocols, especially for routing and control procedures
- Easily interceptable by unfriendly receivers
- Complex repeater topology problems
- Boggs down under heavy loading and discards packets of information
- Less than absolutely reliable
- Can not support heavy traffic and large packets
- A new technology which is different from other forms of communications
- Does not work well with every protocol used by packet switching
- Requires equipment improvements in I/O interfaces, modems and microprocessors
- Experiences deadlocks and degradations in flow control

This discussion briefly identifies those advantages and disadvantages that must be considered before any large-scale network is implemented. A designer of a system must maintain an open mind to the current technology, and weigh the effects carefully between his choices. Packet radio uniquely offers a challenge to overcome the natural and man-made obstacles to this new radio broadcast system.

Attributes for a Practical Packet Radio Network

Adhering to Interpretation (2) of Computer Communications establishes the basis for a model of a network consisting of many low-cost repeaters. This creates a backbone for multiple station communications which can be referred to as RADIONET. In comparison the original ALOHANET was a single station network supported by a few repeaters.¹⁷

The computer communication concept could support either data and or digital speech communications. But limitations on a military network to extremely short bursts will severely handicap the implications toward speech. Target requirements of a network should closely resemble real-time compact information like that which might be sent in an emergency action message (EAM).

The following is a list of capabilities and services that should be considered to support real-time interactive communications between a computer host (station) and user terminals in a RADIONET. A short discussion of each serves to set the stage for those technical considerations crucial to the establishment of a practical military packet radio network.

Frequency Band

The characteristics of radio frequency, (RF), limit use of the spectrum due to the nature of radio systems. For the military this presents one of the two

major obstacles in the broadcast medium. The useable spectrum is a limited resource subject to interference and propagation anomalies. Noise generated by the atmosphere, space sources, or man-made devices must be included in the design constraints of radio equipment. RF propagation is subject to reflection, refraction and diffraction causing a general phenomena called fading. Forms of precipitation such as snow, rain, hail, fog, etc. contribute to path losses or propagation constraints which affect different frequencies in various forms. The effect of any one of these will have a major impact on design of a packet radio network. It is therefore important to select a frequency band that would be practical for the operational characteristics of a packet radio system. This includes a band which allows an optimum RF bandwidth to RF center frequency ratio (\ggg .3), that is not heavily allocated to other systems, and which is not subject to significant propagation path loss.¹⁸

The consideration of frequency is therefore a key attribute for packet radio network design. Research on each of the factors (propagation, multipath and noise) to include packet lengths and delay has established lower and upper limits for a practical packet radio system.

They are as follows:

- The upper VHF Band from 200 MHz to 300 MHz
- The UHF Band from 300 MHz to 3 GHz
- The lower SHF Band from 3 GHz to 10 GHz¹⁹

Chou summarizes the characteristics of RF communications in these three bands as follows:

VHF 30-300 MHz	Broadcast, point to point, VHF television, FM radio land and air mobile	Line-of-sight range Bandwidth = 5 KHz-5 MHz Moderate to low noise and interference Small antennas
UHF 300-3000 MHz (microwave)	Local broadcast, point to point, UHF television, radar, space telemetry	Line-of-sight range Bandwidth to 20 MHz Low noise; local congestion in some regions Small antennas
SHF 3000-30,000 MHz (microwave)	Point to point, terrestrial and satellite communications, radar	Line-of-sight range Bandwidth to 500 MHz Low noise Narrow antenna beam widths ²⁰

By setting a lower limit to the upper VHF band, multipath effects are reduced to a few microseconds and data rates on the order of 100 Kbps or greater can be achieved. The upper limit of 10 GHz for a ground-based packet radio system is primarily established due to the high attenuation caused by the atmosphere and precipitation.²¹ The additional factor mentioned, for allocation of spectrum to other systems in these three bands, is not considered in this discussion of frequency. The next topic, coexistence, will address this attribute.

Coexistence

Although a subtopic of frequency band, the consideration of coexistence potentially must be viewed as a major attribute of a packet radio network in its own

right. By definition coexistence implies the sharing of a common frequency with other users of the band. This implies that several systems (possibly different) can coexist without interference, providing a vehicle for greater spectrum utilization, and introducing a new technology to be geographically implemented.²²

Robert E. Kahn introduces four advantages of shared frequency bands:

1. That certain equipment for different systems can be made compatible at the digital level allowing internetting to be conveniently achieved, if desired. This capability could have striking economic impact in situations where separate radio nets with separate equipment and separate frequency bands are currently established. With common equipment types and a common band, the separation could be achieved via packet labels rather than by using different bands and incompatible equipment.
2. That shared operation can result in better utilization of the frequency spectrum.
3. That the system may be introduced into a band which is currently assigned to one or more other users without first requiring the other users to vacate the band without mutual interference.
4. That the system shall inherently be capable of providing some degree of protection against unwanted interference. Spread-spectrum signaling can assist in achieving this objective and is desirable for antijam communications.²³

The potential of coexisting systems also permits networks to be intermingled over the same geographic area. Within the military, coexisting logistical, and command nets for various operations (land, sea, and air) could provide separate yet compatible communication capabilities.

Such a capability inter- and intra-service allows a coordination never before achieved among a military force.

Transparency

To achieve a network with minimal constraints, no modification of information content should be permitted. A transparent network is one which sends data end-to-end without modifications and as a result optimizes the internal flow of traffic. The packet radio network would appear as a direct connection between the user and the destination.

The user will be concerned with supplying addressing information and control for each packet of data to be transmitted. Once inserted in the network, control would be turned over to the network as a whole to augment routing and delivery by network protocols. Subsequent network reconfigurations or extensions will prove less of a delay if the basic operation of the network is transparent. This is particularly important to a military network since it would affect the overall packet radio network efficiency and reliability.²⁴

Tactical Operations Versus Mobility

Tactical operations should be distinctly defined from mobility because of the crucial implications tied to a tactical military application. While mobility is

important to a packet radio network, it omits the unfriendly environment of wartime operations.

Packet radio component parts of the system must be able to operate while moving at vehicular ground speeds and at speeds in excess of a thousand miles per hour for interaction with high speed aircraft. The mobility requirement associates operations within a specified area of coverage. This includes conducting mobility exercises that consider the effects of the Doppler shift and timing within the boundaries of a RADIONET. Inclusive of the mobility requirements is the need for reasonableness in size, weight and power consumption of the individual parts of the network. Technological advancements in transistors and integrated circuits, and now very high-speed integrated circuits (VHSIC), have advanced the capabilities for meeting these mobility requirements. The resultant system, designed specifically for mobility, is one that operates in any vehicle and whose method of utilization is the same for fixed or moving users.²⁵

The tactical environment must consider radio-electronic combat (REC). A packet radio used in this environment must be antijam and free from spoofing or direction finding. This goes back to the fact that there are two obstacles to the military's use of broadcast medium; the lack of available spectrum and the alterations of electromagnetic waves that destroy the

information contents. In a battle environment, the enemy will try to deny friendly forces the use of the spectrum. The techniques called electronic-counter measures (ECM) are those techniques which deny the enemy's efforts to destroy the information contents during communications. In response, the enemy employs techniques to overcome the obstacles by using electronic-counter-counter measures (ECCM). Each time a 'C' is added by one side or the other, a new or improved method is used to either prevent the destruction of information or cause the destruction of the information content. Hence we face a tactical environment common to military operations. Packet radio as a broadcast medium must be able to operate in this environment for military applications. Therefore a key attribute of packet radio networks is its ability to be mobile and free from enemy interruption.

Rapid and Convenient Deployment

Several features of a packet radio network can be added to insure the contingent of being able to move quickly and easily at a moment's notice. The deployment capabilities of a packet radio network, while part of the mobility requirements, serve to provide time criteria whereby ratings can be established for various threats.

One method to avoid excessive alignment requirements is to use omnidirectional antennas. The radiation pattern of omnidirectional antennas provides a desirable area coverage for mobile terminals and reduces installation complexity. For example, a small team (two or three members) can erect a GRA-4 whip antenna in ten or fifteen minutes. The same antenna can be disassembled in five minutes. This antenna would be useful in a repeater role since it provides additional height above a vehicle-mounted whip antenna. In specific cases, a directional antenna may be required for low-power terminals. Such antennas would be small, and be easy to align through the use of a strength measuring device. They could also be hand-maneuvered to reach different located repeaters/terminals.

The convenience is enhanced if only the mounting of the packet radio terminal is required. A typical tactical teletype operation requires hand-tightened screws to be used for equipment transportation. When the location is reached for set-up, the screws are again hand removed and the equipment pulled out of a ruggedized, compartment-mounted case. Contacts are immediately made when locked in the out position, and cables using quick-connect are locked to the antenna and the power source. Once the set is turned on, it provides immediate

radio connectivity and establishes routing based on the connectivity with a source or sources. In this same manner a packet radio network is self-initializing and self-organizing.²⁶

Unattended Operation and Reliability

The message receiving capability should not be limited by requiring manned-operation. Furthermore such procedures as self-initiation, self-organizing, debugging, restart and shut-down operations, if not automatic, should be capable of being done remotely. The system should be able to run on its own during normal operations, requiring only minor maintenance adjustments with a mean time between failure of at least 1000 hours. A desired network connectivity should be 99.5 percent or greater, with less than .5 percent of the nodes unable to communicate with the rest of the network.²⁷

One parameter limiting the network is the provision of power. A method to increase power availability can be designed into the system to maintain terminals in standby while no packets are being exchanged. Smaller elements in the network, such as the hand-held devices, may only have battery for two hours or less. A battery pack can increase this to twelve to twenty-four hours. The backbone of the network must be able to operate much greater periods without servicing. The repeaters should

be able to operate weeks or months between replenishments of the power supply. The use of rechargeable batteries, like those used in an automobile, can be operated from alternators. Use of small gas or diesel generators can provide five to ten kilowatts of non-fluctuating power for months at a time without servicing, other than refueling operations. In built-up areas such as the Continental United States, battery units can provide power up until a recharge point is reached, then automatically be charged from existing power lines which are downconverted into a charging unit. This eliminates maintenance, other than to replace spent batteries, which may last months to years.

Area Coverage and Connectivity

Two specific attributes of a ground mobile radio network are the coverage area and its connectivity performance in the coverage area. A design diameter of one hundred miles has been suggested, because it would provide good reliability for a packet radio network operating at several hundred kilobits per second.²⁸ A network should be allowed to expand or contract and permit connectivity between any users without prior knowledge. The limiting factors on a packet radio network are the end-to-end delays caused by expansion over too large an area, or the addition of mobile users beyond

system capacity. However the necessity to connect user and resources without prior knowledge about system architecture is important and will increase the usefulness of the packet radio network.

Traffic Handling and Error-Free Performance

ALOHANET has provided extremely useful data to indicate practical packet lengths. In the operation of pure ALOHA packets were designed for a fixed length of 704 bits and generated at 9600 baud. The fixed length was based on the user delays and helped to simplify the system.²⁹ Experimental evidence conducted on RADIONET throughput and delay recommended a maximum fixed-length packet size of several thousand information bits and the possibility for including variable length packets in subsequent networks. For an interactive system, packets of less than 1000 information bits were a more satisfactory choice. They demonstrated average delivery times of 0.1 seconds within a 100 mile coverage.³⁰ Some allowances must be included for smaller packets which provide signaling characters between the portable digital terminals and the host computer. Another method might be implemented by accumulating the data until transmission size is reached, at which time the packet would be transmitted.

While throughput and delay are important measures of traffic handling, so then is error-control

vitally important for computer interaction. The objective of a packet radio system would be error-free performance with a target of an error occurring less than one in 10^{10} packets. While this may seem strident, one should realize that data integrity is crucial to computer operations.³¹ A single error in an emergency action message (EAM) may be responsible for severe loss of life and/or military resources. An entire file of incoming data may be rendered useless or be interpreted wrong by leaders trying to evaluate timely information. Error control can be accomplished by error detection mechanisms and retransmissions, or by a forward-error correcting code to facilitate network flow in one direction. The possibilities for error control mechanisms are endless and can become extremely complex.

Other

The list of attributes important to a packet radio network include other considerations such as inter-netting, routing options, addressing options, resource allocation, directories and virtual subnets, etc. It would be difficult to describe each in detail and account for every possible situation. The essential attributes for a packet radio network are in an early stage of test and evaluation. Specific parameters such as throughput, delay, cost and reliability are classically applied to any technology. But packet radio is

not classical in nature, and has some different attributes not considered in past studies. Several of those not examined fully for a packet radio technology include inherent system overhead, throughput pressure, packet losses, and optimum packet size. Each topic by itself is one that could command at least a volume of evaluative results and still require more study. The compiled list of packet radio attributes described in this paper serves to wet the appetite of those wishing to understand the technical characteristics of a packet radio network. The situation is further complicated by the nature of the military environment and the additional requirements necessary for its success in that environment.

NOTES, CHAPTER 3

¹ Stanley C. Fralick and James C. Garrett, "Technological Considerations for Packet Radio Networks," AFIPS Conference Proceedings, Anaheim, 1975, p. 233.

² Franklin F. Kuo, "Panel on Military Data Networks," Sixth Data Communications Symposium, Pacific Grove, November 27-29, 1979, p. 229.

³ Wushow Chcu, ed., Computer Communications Volume I Principles, Prentice-Hall, Inc., 1983, p. 2.

⁴ Communications Standard Dictionary, s.v. "data terminal equipment."

⁵ Ibid., "data sink."

⁶ Ibid., "data-circuit terminating equipment."

⁷ Ibid., "antenna."

⁸ Chou, p. 1.

⁹ Chou, p. 2.

¹⁰ James Martin, Telecommunications and the Computer, Prentice-Hall, Inc., 1976, p. 3.

¹¹ Stanley C. Fralick and David H. Brandin, "Digital Terminals for Packet Broadcasting," AFIPS Conference Proceedings, Anaheim, 1975, p. 257.

¹² Howard Frank, Israel Gitman and Richard Van Slyke, "Packet Radio System--Network Considerations," AFIPS Conference Proceedings, Anaheim, 1975, pp. 218-219.

¹³ Robert E. Kahn, Steven A. Gronemeyer, Jerry Burchfiel and Ronald C. Kunzelman, "Advances in Packet Radio Technology," Proceedings of the IEEE, November 1978, p. 1477.

¹⁴ Robert E. Kahn, "The Organization of Computer Resources into a Packet Radio Network," IEEE Transactions on Communications, January 1977, pp. 175-176.

¹⁵R. Binder, N. Abramson, F. Kuo and D. Wax, "ALOHA Packet Broadcasting--A Retrospect," AFIPS Conference Proceedings, Anaheim, 1975, p. 214.

¹⁶Roy D. Rosner, Packet Switching, Lifetime Learning Publications, 1982, pp. 9-13.

¹⁷Kahn, p. 171.

¹⁸Kahn et al., p. 1471.

¹⁹Ibid., p. 1471.

²⁰Chou, p. 160.

²¹Kahn et al., p. 1471.

²²Ibid., p. 1470.

²³Kahn, p. 172.

²⁴Kahn et al., p. 1470.

²⁵Kahn, p. 172

²⁶Kahn et al., p. 1470.

²⁷Kahn, p. 173.

²⁸Ibid., p. 172.

²⁹Binder et al., p. 204.

³⁰Kahn, p. 172.

³¹Kahn et al., p. 1471.

CHAPTER 4

PROTOCOL CONSIDERATIONS

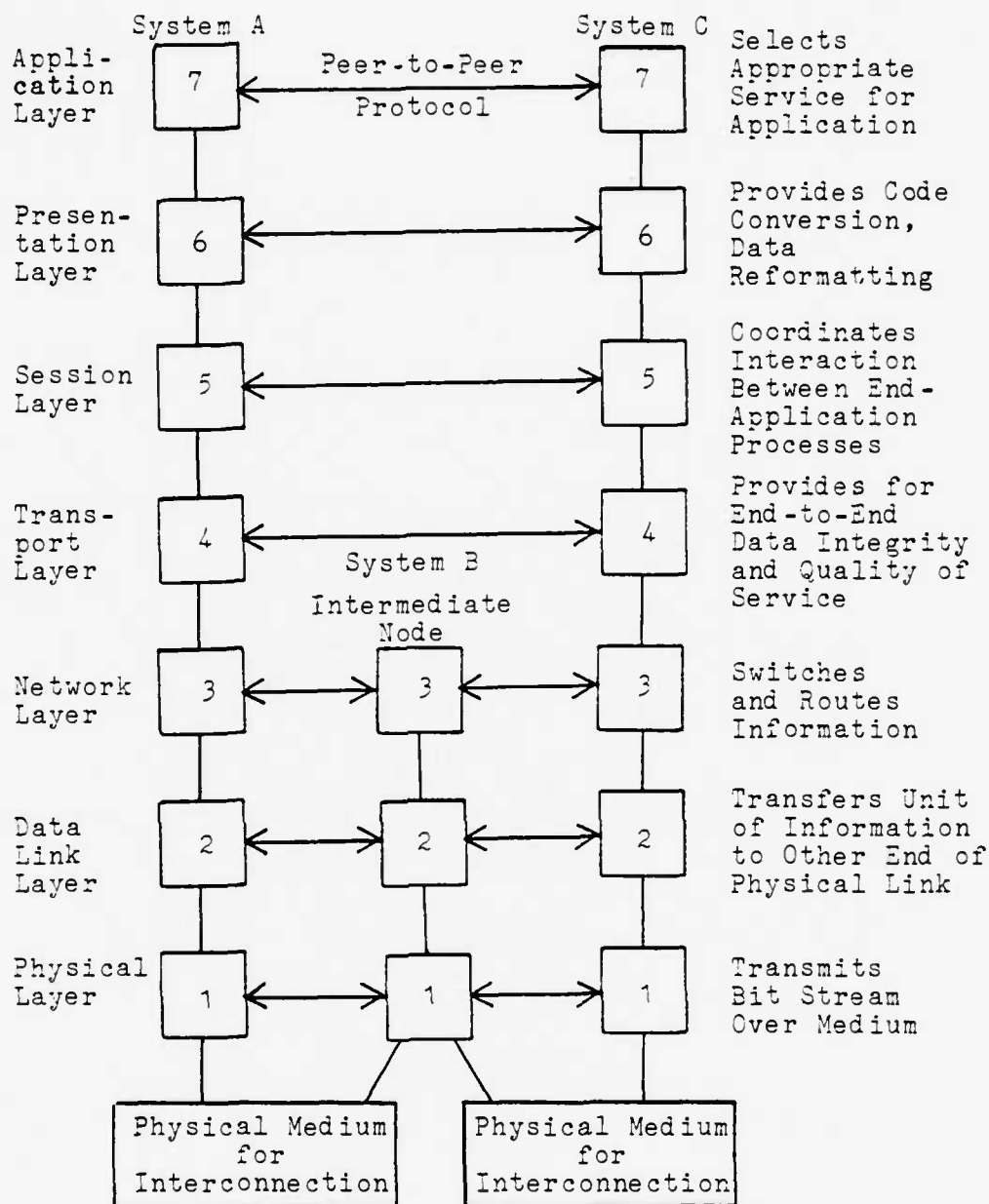
Within the realm of computer communications, rules for transferring data information from system to system must be carefully defined. The DTE-DCE model outlined earlier in Figure 3-1 indicates requirements for interfacing, synchronizing, input/output controlling and commanding, multiplexing, status checking, speed sensing, storing, and assembly/disassembly processing. There are additional functions that would occur in the microprocessor and radio unit as well as other devices which might be added to do encryption. These processes belong to a set of considerations defined by the data flow requirements. For the data transfer to occur fluidly in the network the physical and logical elements must all be defined by the set of rules called protocol.

Standardization of protocols invariably meet obstacles due to the divergent interests between countries, within nations, and even among the multitudes of corporations and standard setting organizations. There are five major organizations which have tried to establish a generalized model for protocol layers. They are:

1. International Standards Organizations (ISO), a cooperative venture of more than seventy member nations. Figure 4-1 is a representation of the reference model which ISO has devised for protocol layers.
2. Consultative Committee for International Telephony and Telegraphy (CCITT), a cooperative venture in which most countries hold membership under United Nations arrangements. (This organization is responsible for the X.25 packet-protocol standard, which standardizes levels 1 through 3.)
3. American National Standards Institute (ANSI), a well-recognized body that has published numerous national standards on a variety of subjects (the body through which the United States participates in ISO).
4. Electronics Industry Association (EIA), a trade association of U.S. electronic-equipment manufacturers, which has produced a variety of industry standards, notable among them the RS-232C standard for attaching a terminal to a computer.
5. The Institute of Electronic and Electrical Engineers Local Network Standards Committee.¹

One of the more well-known reference models was developed by the ISO called the Open System Interconnection (OSI), portrayed in Figure 4-1. The seven-layer model defines the network function in a hierarchical architecture. The major principles of the reference model are described as follows:

1. A layer should be created where a different level of abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.



Source: Gilbert Falk, The Structure and Function of Network Protocols, ed. Wushow Chou, Prentice-Hall, Inc., 1983, p. 39.

Figure 4-1 ISO Open System Interconnection Reference Model

5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.²

Each layer of the OSI reference model represents a distinct protocol in the overall design of a network. The exchange of information moves up and down the seven layers and the units of exchange vary accordingly. For example the top four layers of the model (four through seven) exchange information in the form of message units. At the network layer, sometimes called the communications subnet layer, the units of exchange are packets. Once in the data link layer, frames become the unit of exchange and finally the physical layer concerns itself with transmitting raw bits over the communication channel.³

The subnet layer of the ISO/OSI reference model, beginning at the transport layer, represents the intranet operations through intermediate nodes. System B in Figure 4-1 represents the functions of the internal subnet protocols. The interface requirements in these layers, beginning with host-host consideration in layer 4, must be carefully analyzed for the internal protocol applications to work effectively in a military packet radio network (the X.25 packet-protocol standard).

ARPANET, which has been under the direction of the Defense Communication Agency since July 1975, has established a protocol layering of its own. This struc-

ture can be seen in Figure 4-2. Notice that individual layers represent corresponding applications by the ARPANET. The first four layers serve similar functions to the first four layers in the ISO/OSI reference model with relatively little deviation. Beginning at the end/end subscriber layer the protocol options by ARPANET are less similar to the ISO/OSI model, since they were designed more to satisfy established military requirements. This fifth layer in the ARPANET protocol model contains two main protocols. One, the Network Control Protocol (NCP) was the first interprocess (process-to-process) communication protocol built by ARPANET. The Transmission Control Protocol (TCP), the second significant protocol used by ARPANET, is used in experimental packet radio networks since it was designed to operate for the benefit of a multinet environment. The TCP can provide a sequenced message service or a datagram service for less reliable and unsequenced service as might be true of a packet radio network. The two remaining protocols at this layer, NVP/NVCP, were developed for the experimental Network Voice Protocols and Network Voice Conferencing Protocols. Both run on a datagram service in support of digital, compressed, packet speech. The higher level utility protocols are composed of TELNET and the File Transfer Protocol (FTP) both of which are terminal/host protocols. At the application layer are provisions for remote job entry and electronic mail

APPLICATION	RJE	ELECTRONIC MAIL	
UTILITY	TELNET	FTP	
END/END SUBSCRIBER	NCP	TCP	NVP/NVCP
NETWORK ACCESS	PERMANENT VIRTUAL CIRCUIT		DATAGRAM
INTRANET, END/END	FLOW CONTROL, SEQUENCING, MESSAGE REASSEMBLY		
INTRANET, NODE/NODE	ADAPTIVE ROUTING, STORE AND FORWARD, CONGESTION CONTROL		
LINK CONTROL	NON-SEQUENCED, MULTI-CHANNEL ERROR CONTROL		

Source: Vinton G. Cerf and Peter T. Kirstein, "Issues in Packet-Network Interconnection," Proceedings of the IEEE, vol. 66, no. 11, November 1978, p. 1391.

Figure 4-2 ARPANET Protocol Layering

protocols. For these higher levels a device called the Terminal Interface Message Processor (TIP) is attached to the packet switched computer (called the IMP, Interface Message Processor) for better terminal handling capabilities. This is unique to the ARPANET because terminal handling is required so frequently.⁴

There are many other models that have been designed with the same effect on protocol layering as the ARPANET and ISO/OSI reference models. A standard designed by International Business Machines Corporation (IBM) called Systems Network Architecture (SNA) consolidates philosophies and access methods into three basic functions: Link Control Functions (dynamic link scheduling and error control); Path Control Functions (selecting the communications link); and Transmission Control Functions (identifying the origin of a message and its intended destination). The SNA model has been very successful partly because of the influence exerted by IBM, and most significantly because it recognizes and defines the layers more simply than many other models.⁵ The Xerox Corporation's ETHERNET model has been extremely successful and in many instances is referred to as the industry defacto standard. The significance of ETHERNET to packet radio is its application of datagram service. Only at the host level is virtual circuit used, which makes it a good choice for packet radio applications.⁶ Other models include TYMNET, PTT networks (e.g. TELNET,

TRANSPAC, DATAPAC, and EURONET), Digital Equipment Corporation's DECNET, Wang Corporation's WANGNET, and even several generic protocol layer models created by multiple research sources. Figure 4-3 represents four of the major protocol models with approximated correspondence between each level. The list of possible standards in these four examples alone clearly represents a challenge for scholars, businessmen and governments to make the perfect choice.

Applications

In the application of a Digital Termination System (DTS), indicated as a source for packet radio, the protocol options for a packet radio network have already been breached. Applicants for DTS can be categorized in seven areas as follows:

1. Domestic satellite carriers (Satellite Business Systems, Western Union, RCA) and resellers (ISA Comm)
2. Value added carriers (Tymnet, Telenet, Uninet/ISA Comm, Graphic Scanning)
3. Specialized common carriers (MCI)
4. Telephone companies (GTE Telenet, United Telecommunications/ISA Comm)
5. Computer service bureaus (Control Data/Data Source Inc., Tymshare, United Information Services/ISA Comm)
6. Multipoint Distribution Service carriers (Tymnet/Microband, Graphic Scanning, Contemporary Communications)
7. Entrepreneurs (National Microwave Interconnect Co., Digital Termination Service Inc.)⁷

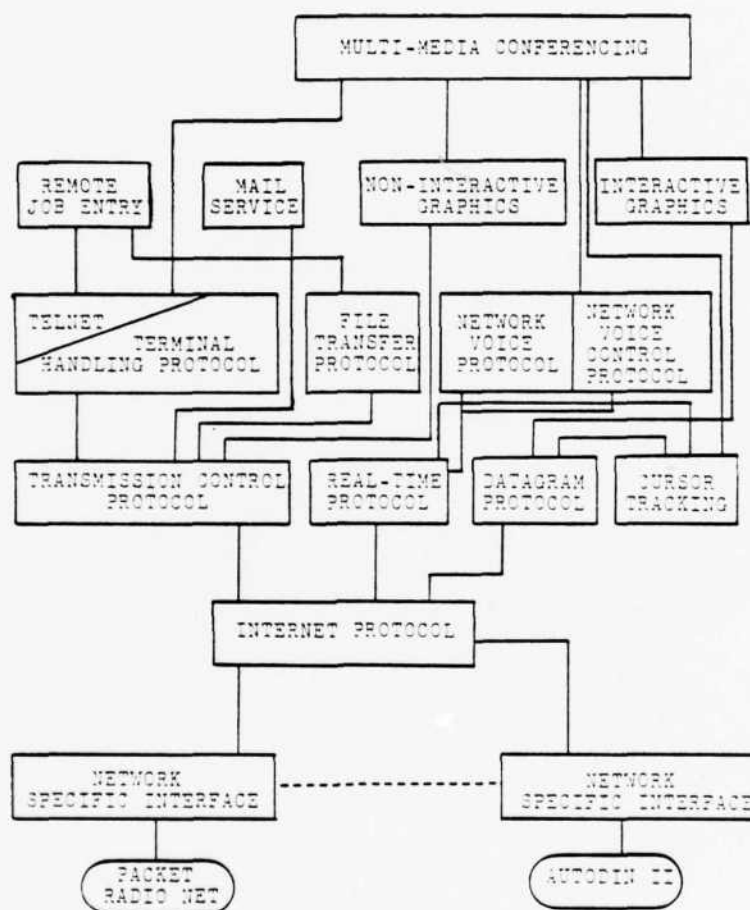
Layer	ISO	ARPANET	SNA	DECNET
7	Application	User	End user	Application
6	Presentation	Telnet, FTP	NAU services	
5	Session	(None)	Data flow control	(None)
			Transmission control	
4	Transport	Host-host	Path control	Network services
		Source to destination IMP		
3	Network	IMP-IMP	Data link control	Transport
2	Data link			
1	Physical	Physical	Physical	Physical

Source: Andrew S. Tanenbaum, Computer Networks, Prentice-Hall, Inc., 1981, p. 22.

Figure 4-3 Approximate Correspondences Between the Various Networks

The seven categories of DTS applicants represent possible sources of interconnection with a packet radio network. Each have been able to foresee the capability of applying a protocol model in order to connect their networks with long distance transmission via packet radio interfacing (DTS). Working systems with proven capabilities for interfacing to the Radio Packet Communication System (RAPAC) include the ETHERNET, Tymnet, Inc., Manhattan Cable, Viacom Cablevision, Inc. and Satellite Business Systems.⁸ Although most applied a virtual circuit, internal net protocol, systems such as ETHERNET used working datagram services (again which might be more easily applied to packet radio).

The significance of the ARPANET protocol reference model centers on the fact that its goals (since July 1975) adopted a purely military viewpoint. Although operationally unsecure, many of the experimental offshoots of the ARPANET stress security and survivability. The satisfaction of providing ARPANET as a purely military, common-user packet-switched network is planned for the proposed Defense Data Network (Schedule shown in Figure 2-8). Figure 4-4 models the protocol architecture designed in 1979 when Autodin II was on the drawing board. DDN will take its place. Network specific interfaces allowed interconnection to the packet radio network in an effort to provide interoperability between all DOD packet technology networks. The Department of Defense



Source: Franklin F. Kuo, "Panel on Military Data Networks," Sixth Data Communications Symposium, Pacific Grove, November 27-29, 1979.

Figure 4-4 Possible Protocol Architecture Layout for Future DOD ARPANET Usage

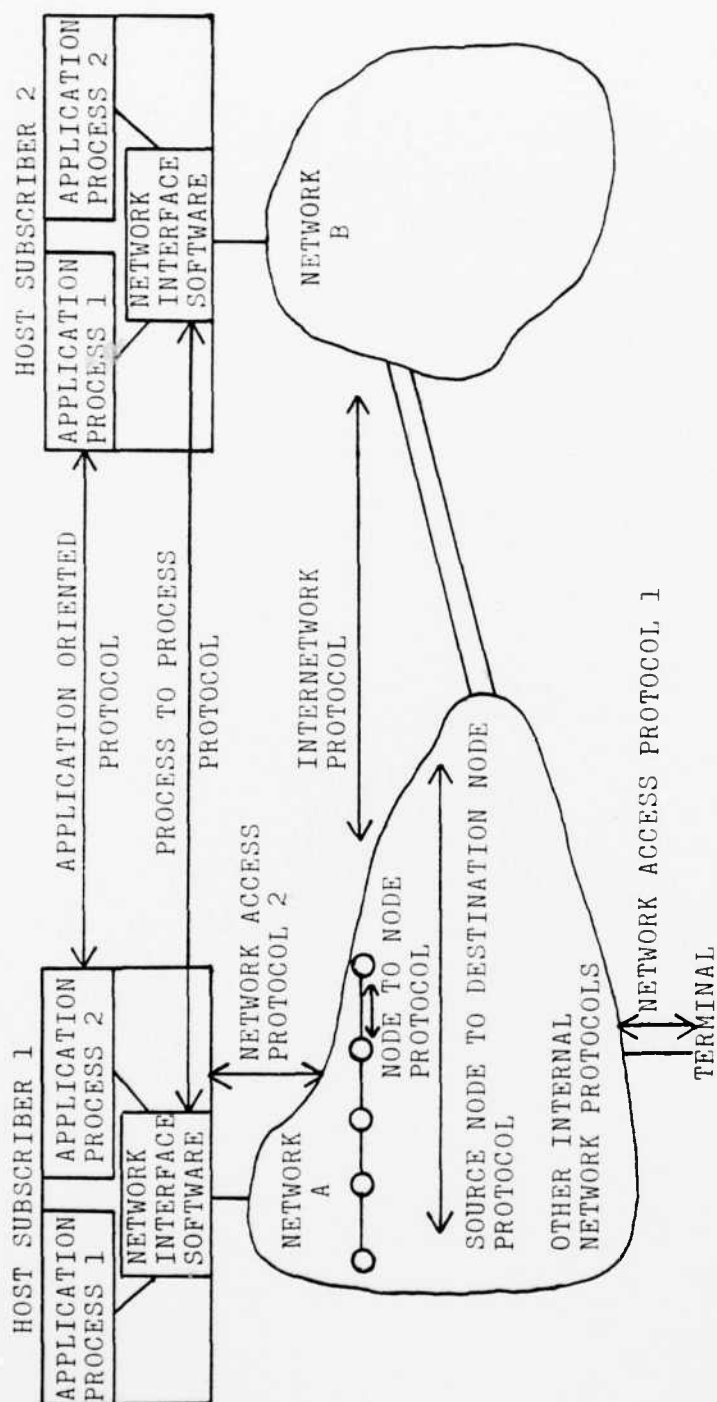
in its search to provide interoperability among diverse military automated systems adopted a Department of Defense Instruction 4120.20 (DODI 4120.20) which sets forth the goal of standardization of protocols. While ARPANET protocol layers are indeed unique, the directives for future growth espouse a need for convergence with industry and international standards.

Untangling the Maze

While protocols may seem a maze at times, reality forces each of the protocol applications, such as DTS and ARPANET, to the same general need for putting their theoretical model into a practical protocol model. This model must answer basic network questions such as how to deal with mechanical, electrical and procedural interfacing to the subnet. Usually these issues are decided at the physical layer where the network assigns voltage levels to represent bits and physical connectors containing pins that identify transmission characteristics. As the protocol moves up the layers from the physical issues, new questions must be solved. The data link is no longer concerned with just ordinary bits, but now must concern itself with a sequence of bits bracketed by opening and closing flags, called frames. New mechanisms must be established to recognize the boundaries for each frame. Error correction/detection, encode and decode and address functions become extremely important

to the operation of the subnet at this layer and IMP-to-IMP algorithms must achieve reliable and efficient communications at this point. The next layer up the model contains the key for routing the packets of information within the subnet, this is the network layer. Two other very important processes occur at this level: flow control and accounting. Finally at the border of the subnet boundary is the transport layer, where the true source-to-destination decisions are made. Sometimes called the end-to-end layer, it determines the type of service to provide the session layer which is the user's interface into the network. Two very important models are developed at the network layer and carried out in the transport layer. They are the datagram model and the virtual circuit model.⁹ Beyond this point we leave the transport layer and enter the user's layers. This study will only address functions of the transport layers.

Another way of looking at protocols is in the relational model of protocols between networks and within networks as viewed in Figure 4-5. There are five categories of network protocols demonstrated by this figure. They are internal network protocols, network-access protocols, process-to-process protocols, application-oriented protocols and internetworking protocols. They are briefly covered by the next five subtopics.



Source: Gilbert Falk, The Structure and Function of Network Protocols, ed. Wushow Chou, Prentice-Hall, Inc., 1983, p. 41.

Figure 4-5 Relationship Between Network Protocols

Internal Network Protocols

The user of a network never sees these protocols at work (transparent), but their primary goal is reliable and efficient transfer of information. They accomplish two primary functions through two subclass protocols: the data transfer protocol and the network management protocol. The data transfer protocol uses two fundamental switching strategies for movement of user data. The two basic alternatives are the datagram and virtual circuit service. In addition these two strategies can be functionally classified as node-to-node or source node-to-destination node protocols. The second subclass protocol, network management, does not direct the movement of user data like data transfer protocols. It is basically used to maintain the network in a state where reliable information transfer can occur. This function is accomplished by routing, line status monitoring and network control protocols.¹⁰

Network-Access Protocols

This protocol function exists in standards that are known internationally due to their significance in the multivendor environment. They exist at the interface points into public or private networks and determine how a subscriber can communicate with other network nodes to which they are attached. For example the X.25 standard is a recommendation devised at the CCITT which defines the computer-to-network interface (DTE-DCE). Initially

developed only for virtual circuit service, the X.25 standard has been extended to datagram service, which is a significant development favorable to transaction-oriented applications like that which might be used in packet radio. Other significant CCITT standards include X.3 which defines the job which the packet assembler-disassembler (PAD) must accomplish; X.28 specifies the command language between the user and the PAD; and X.29 which is an application-oriented, terminal-handling protocol used to control the PAD from the host. While the international standards are in fact gaining popularity and acceptance there still exists nonstandard interfaces that are in use which were developed prior to the standard protocols. Other nonstandard interfaces exist due to manufacturers, such as IBM, who have designed their own network architectures which can achieve more positive results through tailoring, or common device emulation. Finally, a class of nonstandard protocols which is important to this study are those developed due to the uniqueness of requirements such as military systems. Where factors such as security, precedence and closed communities are considered, the international standards fall short. Tailoring, as is done by many of the larger manufacturers, takes on more relevance and must be shared among all networks that need to inter-operate.¹¹

Process-to-Process Protocols

The process-to-process protocols exist solely to support the end user. While this is a very simplified viewpoint of these protocols, viewing the end user as a process will help to understand why they are important. The transport system acts as the support or basic bridge between users (or processes). A process, through interaction with a local control program, functions as the end-to-end protocol mechanism and therefore is the goal post location of the transport system. Two protocols that are well-known process-to-process protocols are the Transmission Control Protocol (TCP) and Network Control Protocol (NCP) of the ARPANET. TCP, adopted as a possible standard for the DDN, has been a key protocol for the experimental deviations in the ARPA community for inter-networking. The X.25 CCITT standard (which also may be viewed as a process-to-process protocol) now extended to datagram service, and TCP, represent significant protocol adaptations amenable to a packet radio network in the end-to-end (process-to-process) role.¹²

Application-Oriented Protocols

The "high-level protocols"¹³ or "functional-oriented protocols"¹⁴ are based on process-to-process level protocols. Quite simply they are interested in the data content of a message and no longer in the data movement or format. Translations or transformations of the data at the terminal, as a file, as remote job

entry, and in many other functional applications such as electronic mail, graphics, facsimile, etc. are the key elements to an effective application-oriented protocol. The concepts at this level are oriented to the host with little or no real telecommunications requirements.¹⁵

Internetworking Protocols

A major issue in all areas of telecommunications is the interoperability within a network and between various networks. This function proliferates both good and bad press since the possibilities for integrated networks sharing resources becomes more feasible as standards are established. These considerations prompt the efforts of many men, organizations and nations, and are the motivation for efficient, reliable internetworking protocols. A plausible approach to providing interconnections has been functionally described by using gateways. A gateway interprets the address fields, translates between the formats of different protocols, and routes the information to destinations either within a network or to a new gateway. The CCITT has attempted to answer the internetworking question through two standard protocols. The X.25, already discussed, operates internal to a network to provide common network access. To provide the link between different networks, the X.75 standard was devised. These two protocol standards are somewhat specialized since they address

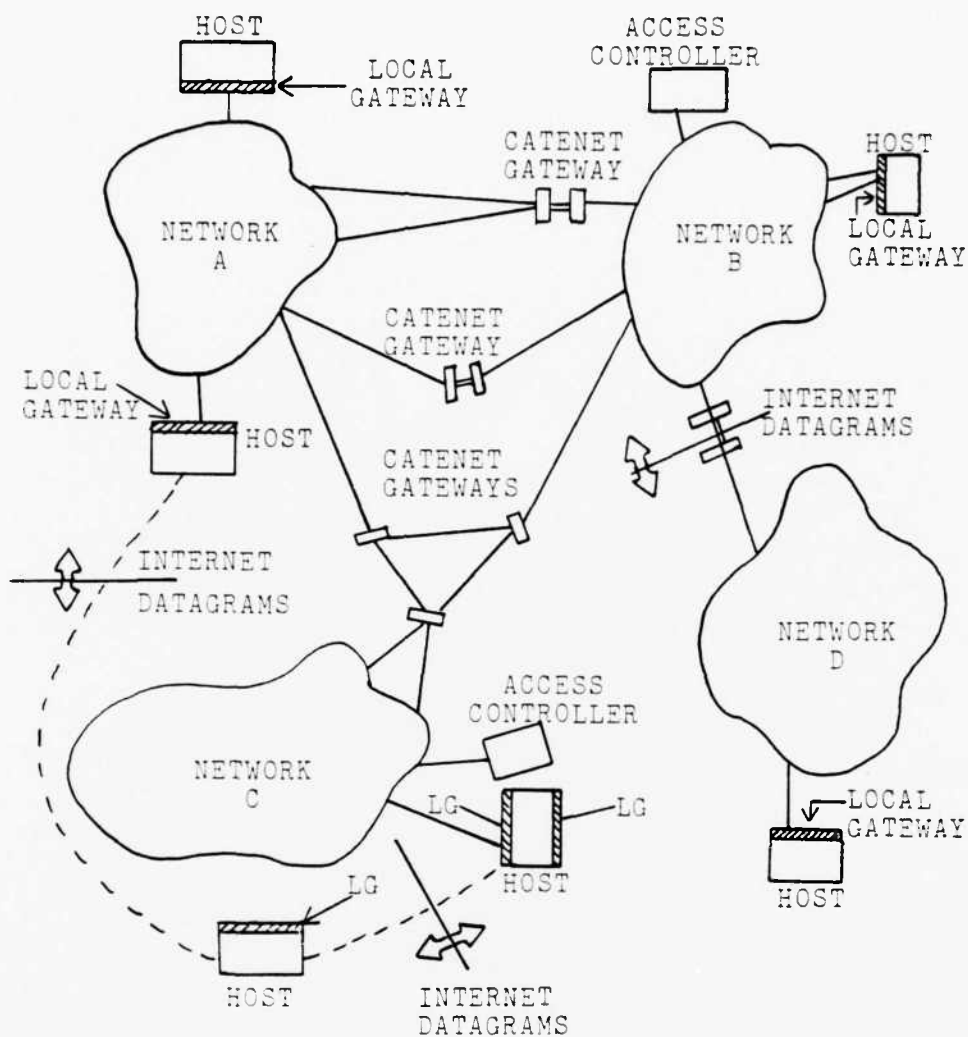
only public packet-switched data networks. But their application offers a guide to the private networks that is very attractive for future implementation.¹⁶

DARPA's attempts at providing packet network interconnection resulted in the catenet model, which is depicted in Figure 4-6. The model is being applied in the five experimental research efforts listed below:

1. Internet datagrams
2. Transmission Control Protocol (TCP) - for reliable end/end transmission
3. TELNET - a virtual terminal protocol
4. File Transfer Protocol
5. Network Voice, Real-Time and Internet Message System Protocols

Four illustrative communications media, the ETHERNET, the ARPANET, packet radio and packet satellite are providing the motivational criteria for DARPA's recent efforts to define an effective internetworking protocol. The crucial advantage for military operations rests on the fact that dissimilar networks would be allowed to communicate, and evolutionary transitions of communications network technology could occur smoothly and cost effectively without interruptions in service.¹⁷

Introduced by L. Pouzin in 1974, the term "catenet" refers to a collection of packet networks which are connected together.¹⁸ The objective of the



Source: Vinton G. Cerf, DARPA Activities in Packet Network Interconnection, ed. K. G. Beauchamp, D. Reidel Publishing Co., 1979, p. 293.

Figure 4-6 Basic Catenet Model

model centers on its ability to interconnect different networks through a set of rules and algorithms. Motivated by the need to interconnect many locally optimized networks and to allow phased technology change of a network without affecting change to the whole network, the catenet model offers packet radio technology the ability to truly become an integral part of a much larger network scheme.¹⁹

Levels of Interconnection

The interconnection of two networks can occur at various levels. The common device to accomplish this interconnection is the gateway. A gateway terminates the internal protocols for each network and provides the necessary translations so that packets move easily from one network to another. There are four basic methods of interconnection for packet networks:

1. Common Subnet Technology. For common subnets, the interconnection is made at the packet level where the internal structure is common to all networks. Gateways, instead of being a device such as a computer, may consist of software routines in the adjacent packet switches which accomplishes accounting, readdressing and specialized access control methods. This arrangement might be typical of a set of military packet radio networks. The network may also use non-duplicative addresses so that the readdressing function is not required at the gateway.

This method is efficient, but not practical in the multi-vendor environment. Typical networks do not allow the interconnection to be made at the packet level. This would be possible for a total system design which might be accomplished within the DOD for a interservice connection of packet radio networks. Connections across packet networks such as ETHERNET, ARPANET, packet radio and packet satellite can not be accomplished by this technology. These four networks use the interconnection approach espoused by the CCITT X.25 standard in the form of common network access interfaces, the next topic.²⁰

2. Common Network Access Interfaces. In this level of interconnection the gateway acts as a termination point of the subnetworks. The node-to-node exchange in common subnets is now identified by a network access interaction. There are two basic types in use: the datagram interface and the virtual circuit interface. A datagram interface allows each packet to be handled separately. The gateway treats each packet independently from all other packets. The virtual circuit interface treats exchanges of information as sessions. The gateway requires exchanges of control information from the user to set up addresses, translation tables, and routes before any data packets can be forwarded. Once the flow of data meets all the gateway requirements the session is established without any other packet identification except control exchanges identifying the close of a

packet series. The datagram and virtual circuit interfaces are distinguished from the datagram and virtual circuit services by the gateway and subnetwork routines. For example, the ARPANET uses datagram interfaces but its subnetwork keeps packets in sequence for delivery at destinations (virtual circuit service).²¹ This relationship can be depicted as follows:²²

		Interface Presents to the Hosts	
		Virtual circuit	Datagram
Method Used	Virtual Circuit	SNA	(Unusual)
Inside Subnet	Datagram	ARPANET	DECNET

3. General Host Gateways. As a general connection of networks, through indistinguishable gateways (from any other network host) it offers the advantage of being able to handle any internal operation whether datagram or virtual circuit. The strategy also permits new systems to interact with older ones and still operate internally with more innovative and efficient designs. The strategy looks at every packet, no matter what its length (up to a maximum), as a datagram host and provides encapsulation or "wrapping".²³ Under this strategy no guarantee is given for delivery or sequenced transmission. Such an interface would easily support packet-voice protocols. There are provisions also for virtual circuit operation which does encapsulation/decapsulation of datagrams, mapping of internet source/destination ad-

dresses into local network addresses, and datagram routing within the gateway. One of the chief disadvantages of a general host gateway is the requirement for all subscribers to implement the same network interface.²⁴

4. Protocol Translation Gateways. Although a general host gateway does some translations (encapsulations/decapsulation), this method employs a more involved strategy. It depends partly on the closeness of protocols used across networks. If the protocols in use do not in some general way resemble each other, then a mismatched protocol interconnection may be forced into extending translations through multiple gateways (devices or software routines). The usefulness of this type interconnect strategy is limited and in practice may be extremely difficult and reduce efficiency below acceptable norms.²⁵

Datagram Versus Virtual Circuit Service

The distinction between datagram and virtual circuit interfaces, and datagram and virtual circuit services was explained in the discussion of the common network access interface. Both datagram and virtual circuit services act as a means of network interconnection based on the user's perception of the network. Other protocol processes occur at the user level which direct the internal protocols in a manner that is either a datagram mode of operation or a virtual circuit mode

of operation. No special internal protocol is required to set-up these functions. It is the characteristics established at each interface which prescribe which mode of operation will occur.

The following comparison is made between datagram and virtual circuit services:

DATAGRAM	VIRTUAL CIRCUIT
Self-contained	Long term
Fully identified	Initially set up and formally terminated
Highly (but not absolutely) reliable	Absolutely reliable
Unsequenced	Sequenced
Uncontrolled	Highly controlled ²⁶

First, a description of the major properties of virtual circuit service is necessary:

1. Sequenced Data Transfer

All data bits delivered to the destination host must be in the same order they were delivered to the network by the source host. This property implies the need for the message reassembly process.

2. Data Transparency

Data bits in the user data fields must be accepted in any sequence of ones and zeros. No sequence may be prohibited, despite the fact that special bit groups are needed to "flag" the beginning and end of packets. This property implies the need for special handling of the data stream to protect against inadvertent flag sequences.

3. Full-Duplex Path

Data has to be able to flow in both directions between the end users simultaneously. Thus the initiation of a connection and buffering for a message in one direction requires a similar process in the opposite direction.

4. In-band/Out-of-Band Signaling

Signals have to move between the users and the switches in order to control the flow of information, to inform the user of status information, to respond to network or user inquiries, etc. This signaling can take place as part of the normal user data stream (in-band) or outside the normal user data transmissions (out-of-band).

5. Flow Control

The network must be capable of reducing the allowed input rate of information. This is important to prevent congestion to the point where normal operation may become impossible.

6. Error Control

All network transmission must be error protected, so that the probability of an undetected network-introduced error will be negligible.

7. Interface Independence

Operation of the network must be independent of the physical and electrical properties of the user interface. It must be consistent with the logical data structures.

8. Switchability

Network operation in the virtual circuit mode allows information to be exchanged among various user pairs by modifying the address field of the user segments.²⁷

In response, the properties of the datagram mode of operation are as follows:

1. Self-contained

The information contained in a datagram is complete and useful in and of itself. It does not depend on the contents of preceding or following datagrams to have utility to the end users.

2. Fully Identified

The beginning and end of the datagram are readily identified by the destination, and are recognizable as a complete entity. Any needed control, numbering, and routing information are fully identified within each datagram.

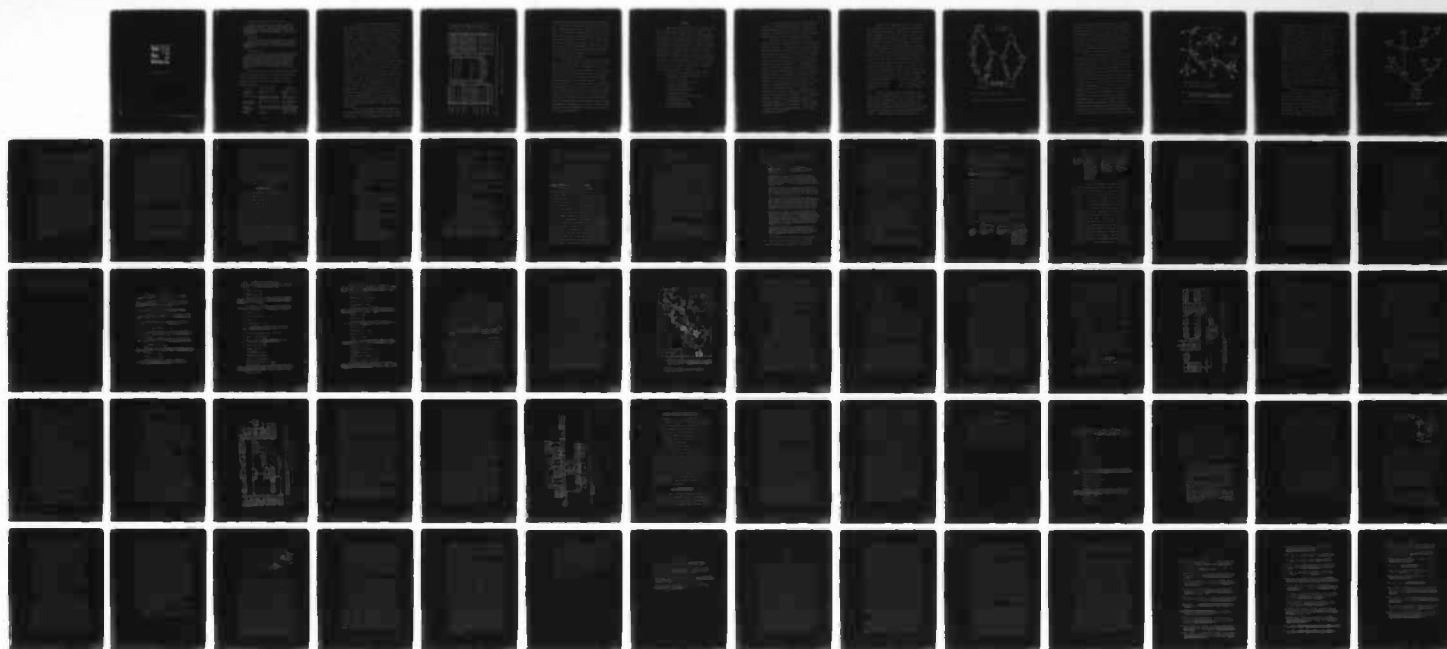
AD-A139 162

A PRACTICAL TERRESTRIAL PACKET RADIO NETWORK(U) AIR
FORCE INST OF TECH WRIGHT-PATTERSON AFB OH
S W PHILLIPS NOV 83 AFIT/CI/NR-83-83T

22

UNCLASSIFIED

F/G 17/2.1 NL



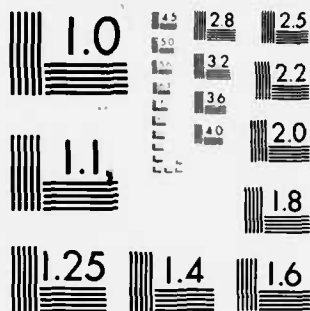
END

DATE

FILMED

5-84

DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963-A

3. Highly (but Not Absolutely) Reliable

Datagram delivery has a very high probability of success. However, there is a chance that one will become lost, with the destination having no knowledge that it has ever been sent. It is also possible that a duplicate datagram may arrive at the destination.

4. Unsequenced

Sequentially transmitted datagrams may arrive at the destination in a different order. Since the datagrams are considered to be self-contained, the network makes no attempt to check or preserve entry sequence.

5. Uncontrolled

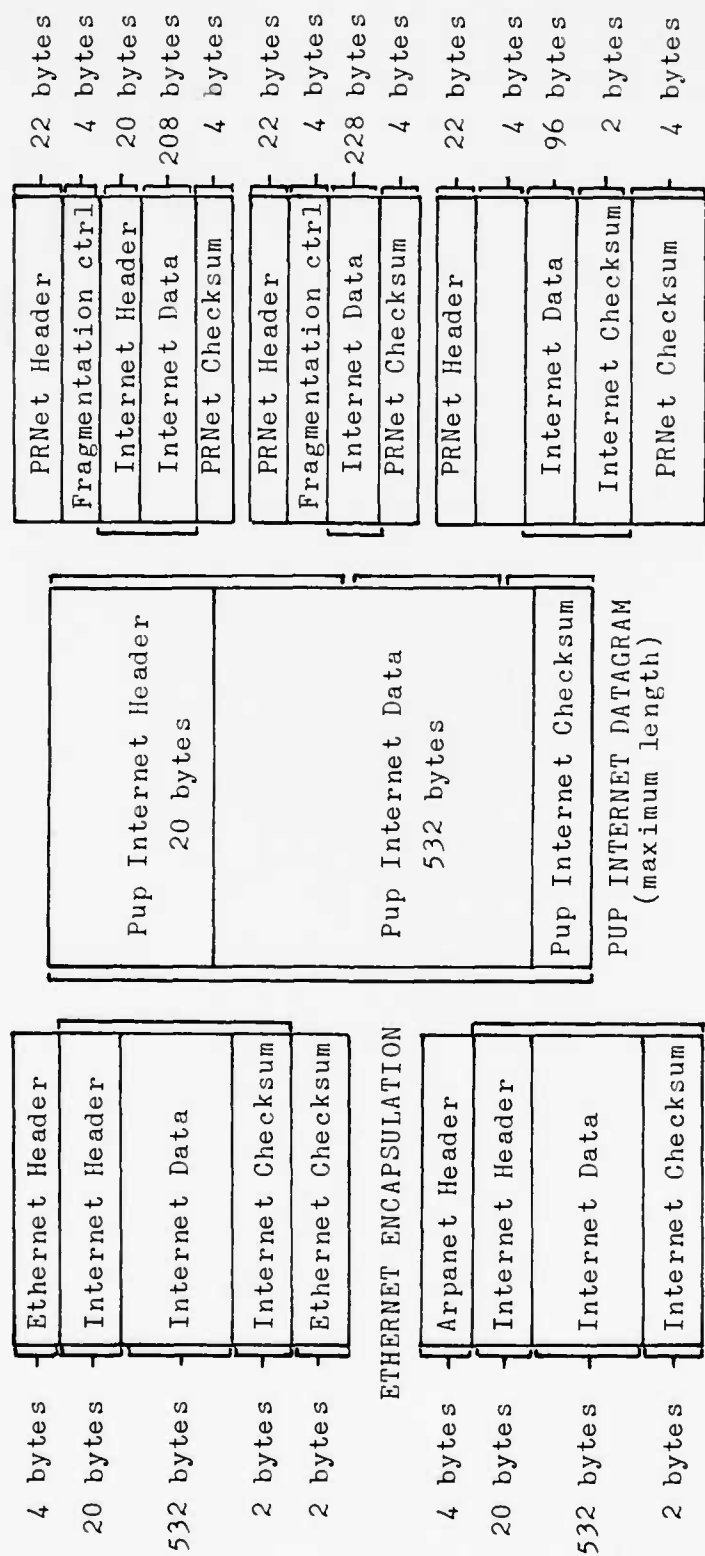
The network will attempt to advise the datagram originator of failures to deliver a datagram or of network conditions that may have resulted in the loss of a datagram. However, after the datagram leaves the source node, the flow is uncontrolled (except for network-induced error checking). It may not be possible for the network to keep the source user informed of the progress of the datagram.²⁸

Finally, it should now be apparent that virtual circuit and datagram services offer two distinct modes that meet individual needs of a network. The major issues between the two modes of operation can be summarized as follows:

Issue	Virtual circuit	Datagram
Destination address	Only need during setup	Needed in every packet
Error handling	Transparent to host (done in the subnet)	Explicitly done by the host
End-to-end flow control	Provided by the subnet	Not provided by the subnet
Packet Sequencing	Message always passed to host in order sent	Messages passed to host in the order arrived
Initial Setup	Required	Not possible ²⁹

An example of a working internetwork architecture using datagram mode of operation is the PARC Universal Packet or PUP. In widespread use within the Xerox Corporation, PUP functions basically as a transporter of datagrams. In dealing with the Department of Defense, Xerox's ETHERNET communications network has been a prime example of what can be done by interconnecting their local-area broadcast channel with the DOD long-haul communication facilities. The PUP protocol hierarchy has implemented a packet transport mechanism which can interconnect to the ARPANET, ARPA Packet Radio Network and a collection of other ARPANET-style store-and-forward networks. Since each of the interconnected networks have distinct native protocols and exhibit as much as three orders of magnitude difference in bandwidth a process of translations in the form of encapsulation is done by the PUP process. This is done by level 0 code of the PUP protocol hierarchy. The transformation of the packets into an internet packet transport mechanism is called a network driver. The performance of the transport mechanisms, as in many datagram systems, is not perfect. The current ETHERNET network using PUP architecture is achieving a packet loss rate of less than one percent and has already been integrated into five major networks nationwide.³⁰

Figure 4-7 shows the encapsulation that has been done between the ETHERNET, ARPANET and ARPA Packet Radio Network. A special arrangement programmed in the



Source: W. R. Franta and Imrich Chlamtac, Local Networks, Lexington Books, 1982, p. 444.

Figure 4-7 Pup Encapsulation in Various Networks

network driver setup for the ARPA Packet Radio Network in the San Francisco Bay area fragments the packet sizes into a smaller maximum packet size of 232 bytes (8-bits each). The performance characteristics in the broadcast medium are less reliable at larger packet sizes. Within the system architecture of the PUP model, packet radio hosts are identified separately from other hosts, since they will not support the broadcast packets of the rest of the system. The lower level driver further breaks out the maximum length datagrams into datagrams the packet radio system can handle.³¹

The proliferation of virtual circuit service is more widely spread compared to datagram service. Virtual circuit, unlike datagram, is independent of the subscriber interface. Even though datagram is more simple and flexible it can not guarantee end/end reliability like virtual circuit and many times datagram relieves momentary congestion by discarding packets. Virtual circuit service will not discard packets since delivery is controlled from start to finish by sending all packets in one session along the same path or supplying sequence numbers to preserve each packet. As a general rule the virtual circuit approach is more complex than datagram since it requires more state information in each gateway. The progress and condition of a virtual circuit is maintained in the state information along with flow control and routing information.³²

Routing

Routing, a chief consideration in a packet radio network, adds to the complexity of the protocols that must be used. With a closed system of a finite number of terminals the routing strategy is not very difficult. Once repeaters (multiple) are added, routing becomes an issue which must be given priority attention in protocol development. The basic issues of routing are based on connectivity, reliability, and efficiency. To assure connectivity, a message packet must be able to start anywhere in the network and reach its intended destination. For a system to be reliable and efficient, the network should be able to support a large number of messages, transmitted with a small time delay.³³

The choices of routing strategies include:

- Flooding or Undirected Routing
- Selective Flooding
- Static or Directory Routing
- Centralized Routing
- Isolated Adaptive Routing
- Distributed Routing
- Hierarchical or Directed Routing
- Broadcast Routing
- Point-to-Point Routing
- Multidestination Routing

An interpretation of any of the single modes of routing may yield distinct algorithms. The simplest routing strategy probably is flooding. Although rudimentary in operation, it can be made workable by placing constraints on the way that flooding is controlled.

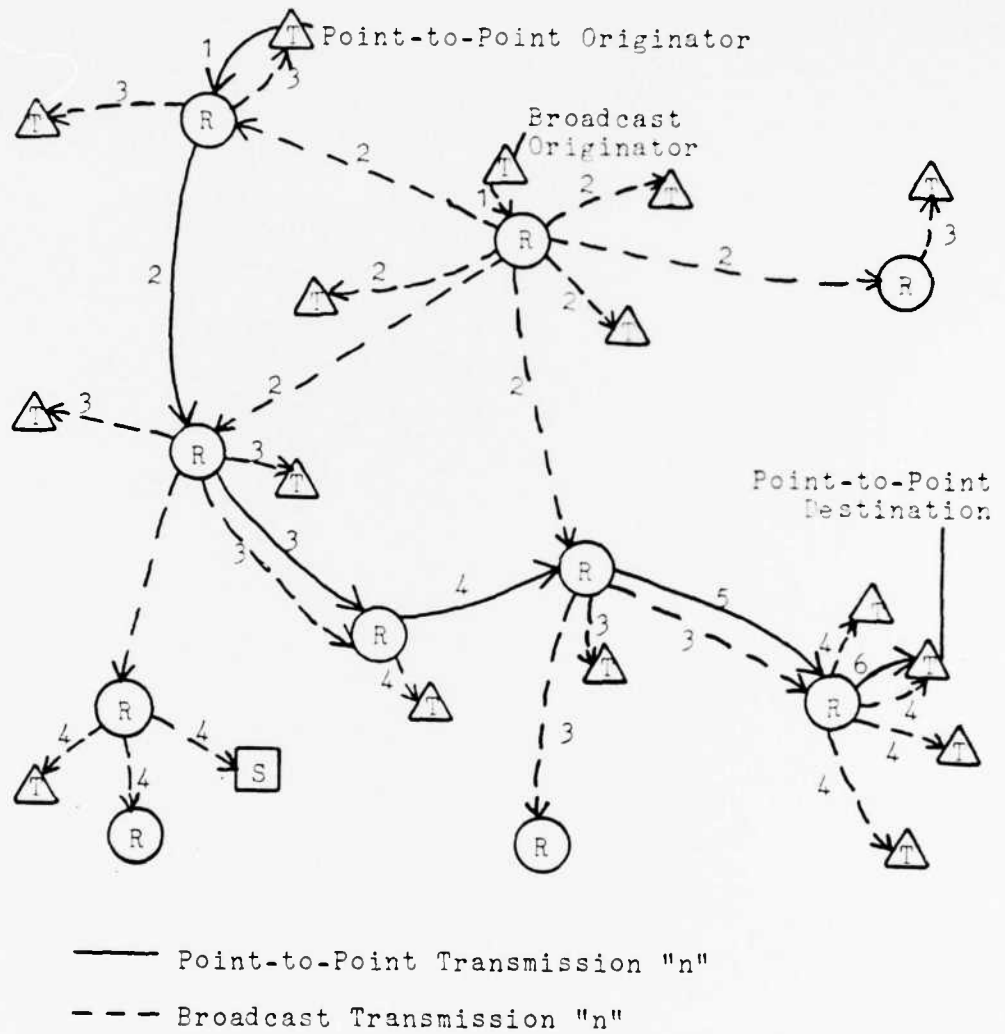
Under the topic of undirected routing, a strategy which uses flooding techniques with constraints can be very useful. A modified flooding version may use single restraints or a combination of restraints, whichever matches the complexity of the network. One of the big problems in using flooding is that a network may receive a packet and successively bounce it around from repeater to repeater indefinitely. This phenomena is known as looping. One method to reduce looping is to attach a value on each packet called the hop counter or handover number. As the packet is bounced around the network each repeater successively reduces the hop counter by one. Once the hop counter reaches zero, the packet is no longer repeated in the network. This process is called packet aging.³⁴ The choice of the initial value in the hop counter is important to the design of the network. If the number is too large the network may find that it's capacity is tied up with arbitrary packets. This decreases the efficiency and handling capabilities of the network. If the number is too small then some packets may fail to reach their intended destinations.³⁵

Figure 4-8 is an example of how a hop counter with a maximum hop number of three might work, without any additional constraints. Central Site 1 (CS1) originates a packet in all directions, which is received by CS2 and Repeaters A and B (RPA and RPB). CS2, RPA and RPB subtract one (leaving two) and resend the packet. CS1 therefore receives its original packet on the second bounce. Also Station 2 (ST2), RPG, RPF, and RPC receive the packet for the first time. All sites subtract one, (which leaves one left) so therefore must repeat the packet for a final time. Once repeated the next receiving units will subtract one (a result of zero in the hop counter) and discard the packet at this point. By using a count of three, the packet was able to reach all participants in the network, but any sites expanded from either ST1 or RPD would not have received the packet. Note that, transmissions were iterated progressively around the originating site. A network operated in this fashion ties up precious resources on needless repetition.

Another useful constraint to implement with flooding is to require repeaters to store each received packet for a finite amount of time. The goal is to again reduce looping. A repeater stores either the whole packet or a portion of the packet such as the header, sometimes referred to as the unique packet identifier, UPI.³⁶ As each successive packet is received, the

fields in each are compared for redundancy. The repeater discards those that it recognizes as rerun packets for the time designated by the constraint. This constraint sometimes places undue requirements on buffer areas. The time factor for holding packets must therefore be carefully analyzed so that the network is not forced with maintaining large storage at each repeater. It must also take in to consideration the network topology and possible expansions or contractions of the same.

These considerations are often part of a scheme identified as broadcast routing. In the broadcast mode, each packet is radiated away from the source radio in an omnidirectional wave. The use of the unique packet identifiers permits the system to continue the flow in the outward direction and stops any repetitions by successive repeaters by discarding formally received packets. Although not a particularly efficient system, and sometimes unreliable, the broadcast mode is a robust method for distributing packets. It is also a system that is generally used for multideestination delivery to all or a subset of the users in the network.³⁷ Figure 4-9 illustrates a broadcast transmission originated at a terminal location. The closest repeater receives the broadcast and similarly rebroadcasts the packet, in a wave-front type of propagation, omnidirectionally. Notice that the originating terminal sending its transmission over route one does not repeat the process, since



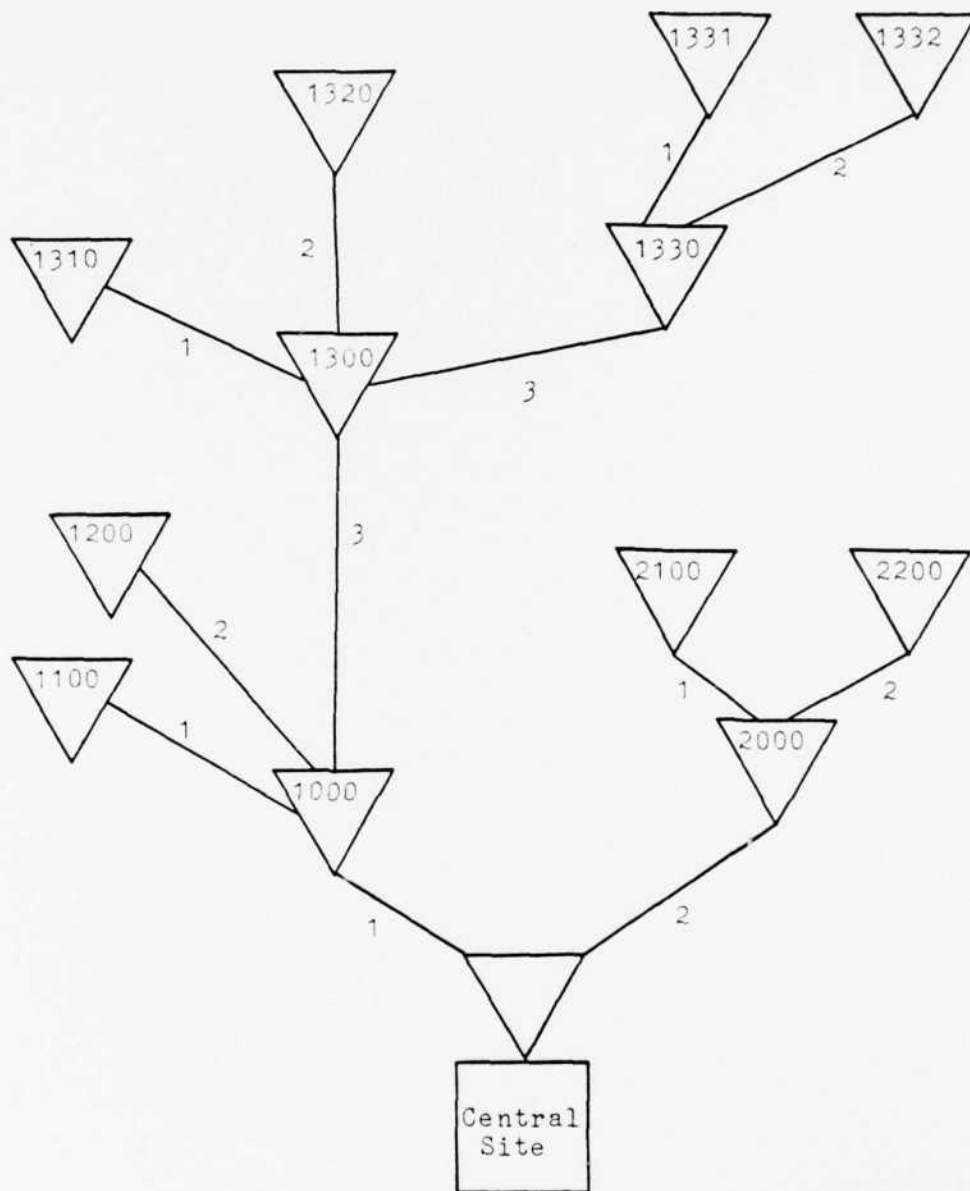
Source: Robert E. Kahn et al., "Advances in Packet Radio Technology," Proceedings of the IEEE, vol. 66, no. 11, November 1978, p. 1480.

Figure 4-9 Point-to-Point and Broadcast Routing

its comparison of the UPI causes it to discard the packet. In addition, the receipt of its own packet from the broadcasting repeater can serve as verification that the packet was sent without error. If the terminal identifies an error in its packet, it can repeat the transmission. The wave-front continues to route two where it reaches three other repeaters who likewise send the packet forward, until finally the point of destination is received by one, all, or a subset of the terminals. This same figure shows a point-to-point strategy which is different from the broadcast routing strategy.

In Figure 4-9 a terminal originates a packet for point-to-point delivery. The closest repeater receives the packet and forwards it to the next closest repeater, and so on, until it reaches the destination terminal. The routing of the packet is by a directed method, and may either be done by the packet or by each successive repeater. This decision is made in designing the algorithm.

The directed, or hierarchical routing algorithm, is a more reliable method of routing strategy (the second algorithm considered useful in packet radio). Labels are placed on every device in the network and the repeaters are organized into trees with the root at a central site, as in Figure 4-10. Several methods exist for deciding the directed route. One method is to have the central site in total control. It therefore would be the only



Source: Andrew S. Tanenbaum, Computer Networks,
Prentice-Hall, Inc., 1981, p. 280.

Figure 4-10 A Repeater Tree Labeling

element which knows the overall system connectivity, and would decide all packet routing through a compiled routing table given to each repeater. Periodically the station would test the network in order to maintain an efficient routing scheme.³⁸ The packet therefore contains the mechanism which moves it through the network in the form of source/destination identifiers. It's header must be able to carry the entire sequence of point-to-point decisions, which is one major disadvantage to using this method, since it causes larger overhead.

Another more useful directed method is operated by allowing the sender to determine the most attractive route. This can be done by using a route set-up packet which moves back and forth through the network in order to inform the sender on each best route strategy.³⁹ The repeaters must take part in this operation in order to find the shortest delays to a given destination. They may accomplish this through random tests of the delay to each repeater within their connectivity. They may also decide normal paths that carry certain addressed packets and discard those that ordinarily are not routed in these paths. Occasional intervention from a station may be required so that paths are not eliminated entirely and to make allowances for times when alternate routing or topology changes occur.

A third algorithm, which is more adaptable to the mobile environment, is achieved by permitting the repeaters to make all routing decisions. Each repeater randomly tests its distance to every other repeater. Once the full circle is complete, a table is compiled at each repeater which gives its distance to every repeater in the network. A hop count line matrix, as in Figure 4-11, can be kept inside the repeaters telling it which repeaters are in range, and giving it a decision capability for routing packets. As packets arrive at the repeater it can numerically check to see if it is closer to the destination than the sender. If it is not closer, it will discard the packet by interpreting that the packet is heading in the wrong direction. If closer, then the repeater will sense that the packet is heading in the right direction, and retransmit it in the network.⁴⁰

An example of this third algorithm can be demonstrated using Figure 4-11. Site I wishes to send a packet to the central site. It knows by this matrix that it is only "two hops" away from the central site. After transmission, sites C, D, H, K and L receive the packet sent by site I. Both sites C and D know that site I is only two hops and that they are three hops from the central site, so they realize that the packet is going in the wrong direction and discard it. Sites H and L, also

two hops from central site, are no closer than I, so they discard the packet. But site K is only one hop from the central site and realizes that the packet is moving in the right direction, so it retransmits the packet to the central site.

Although other routing strategies are available the three described above are considered the most useful strategies for a packet radio network. All three strategies would be amenable to a working military network and offer a solution to the repeater topology problem.

Multiaccess Protocols

Whenever independent contending users share a resource, the need for multiaccess protocols are required to achieve maximum utilization and a high degree of connectivity. The need to share scarce and expensive resources, and the connectivity requirement, are the two major contributing reasons for multiaccess protocols. For the wide area distribution requirements for packet radio, two considerations must be further defined for a satisfactory multiaccess protocol to achieve the desired results: the singlehop or the multihop network. In a singlehop network, like ALOHANET, SATNET or ETHERNET, a single transmission medium is shared by all subscribers. The multihop network combines the features of the singlehop environment with a store-and-forward repeater architecture. An example of this type of network is DARPA's experimental PRNET.⁴¹

Multiaccess protocols can be grouped into five classes:

1. Fixed Assignment Techniques to include:
 - Frequency Division Multiple Access (FDMA)
 - Time Division Multiple Access (TDMA)
 - Code Division Multiple Access (CDMA)
 - Asynchronous Time Division Multiple Access (ATDMA) also known as Statistical Multiplexing (STATDM)
2. Random Access Techniques to include:
 - ALOHA
 - Slotted ALOHA
 - Carrier Sense Multiple Access (CSMA), persistent, non-persistent and p-persistent
 - Slotted CSMA, persistent, non-persistent and p-persistent
 - Busy Tone Multiple Access (BTMA)
 - Capture Technique
 - Spread Spectrum Multiple Access (SSMA)
3. Centralized Controlled Demand Assignment Techniques to include:
 - Circuit-Oriented Systems
 - Polling Systems
 - Adaptive Polling or Probing
 - Split-Channel Reservation Multiple Access
 - Global Scheduling Multiple Access

4. Distributed Control Demand Assignment

Techniques to include:

- Reservation ALOHA
- First-in First-out (FIFO) Reservation Schemes
- Round-Robin (RR) Reservation Schemes
- Minislotted Alternating Priorities (MSAP)
- Assigned-Slot Listen-Before-Transmission Protocol
- Distributed Tree Retransmission Algorithms
- Distributed Control Algorithms

5. Adaptive Strategies and Mixed Mode Techniques such as:

- URN Scheme
- Dynamic Management of Packet Radio Slots
- Reservation Upon Collision (RUC)
- Priority-Oriented Demand Assignment (PODA)
- Mixed ALOHA Carrier Sense (MACS)
- Group Random Access (GRA)

Fixed assignment techniques have the most rigid controls and are nonadaptive to varying demands, whereas random access techniques involve no controls and are adaptive to varying demands. The techniques associated with demand assignment require that precise information regarding the need for the communication resource be

exchanged.⁴² The final category, of adaptive strategies and mixed modes, attempts to either adapt earlier techniques or mix the techniques for the optimum multiaccess for a given requirement.

For this study only CSMA and SSMA will be considered. Both offer the adaptability to a changing environment, good performance, and additional benefits above purely contention models like ALOHA or the rigid models used in fixed assignment techniques.

Spread Spectrum Multiple Access (SSMA)

Probably one of the most promising efforts in multiple access techniques is spread spectrum (SS). As the most common form of code division multiple access, it provides useful applications for satellite communications, mobile ground radio, and computer communication networks.⁴³ It has been under development by the military for sometime, but is just now receiving major attention in all areas desiring better frequency use.

Spread spectrum is a signal processing method which employs considerably more bandwidth than is normally required to transmit information. But the bandwidth area that is occupied, is spread below detectable levels of receivers so that interference is reduced below normal grass-levels of even the most sensitive receiver. This produces a signal that is not only non-interfering, but also offers an additional characteristic which gives it low probability of interception. Spread spectrum techni-

ques come in three basic varieties:

1. Frequency Hop
2. Direct Sequence Encoding or Direct Spread
3. Chirp

The two most common forms are the frequency hop and the direct spread methods. The direct spread technique takes a carrier frequency and phase modulates it with the digital data and a pseudorandom bit stream produced by a bit generator (PRBG). The PRBG produces the spreading signal, since its clock rate, R_c , has a value much greater than the data rate, R_b . The frequency hop method randomly bounces a data-modulated carrier frequency within a known frequency range. The rate of bouncing and the frequency spread produces an illusively modulated signal, which is difficult to jam or intercept. Since signals at the receiving and transmitting nodes are synchronized, the random bounce is known, and thus can be de-spread. The key advantage that either method offers against jamming is that receiver and transmitter are privy to information not known to others and not easily reproduced.⁴⁴

The frequency hop method is a system which has received significant attention in the military. Under tactical environments, jamming of command and control (C2) nets is predictable. Steps have been taken that introduce the frequency hop method in these radios, so

that enemy efforts are less significant during a crisis. The following is a list of characteristics for a frequency-hopped transmission, where N is the number of possible output frequencies:

1. The frequency-versus-time program can be a pseudo-random sequence or code, making it extremely difficult for an unintended receiver to derive any information.
2. Multiple transmitters and receivers can be accommodated within the same overall assigned portion of spectrum by assignment of different codes. Multiple access can be effected by code selection--this is called code-division multiple access (CDMA).
3. If the frequencies are spaced at least as far apart as the bandwidth required to support the information rate, the hopped transmissions will not overlap in the spectrum and the "processing gain" is calculated by $G_p = 1/N$.
4. If the spectrum of interference or jamming is less than the information bandwidth, the system's performance will be improved by the processing gain. This is because the interference enters the receiver only during the dwell time on its discrete portion of the spectrum; hence interference is reduced by the processing gain, G_p .
5. The converse is also true--the time-averaged interference caused by frequency-hopping transmitter to a fixed-tuned (conventional) receiver will also be reduced by G_p . Interference between transmitter-receiver parts, or even networks, operating in the same spectrum space can be kept negligible, or zero, by managing mutual intersections of the codes.
6. Note that, to produce the same signal-to-interference power ratio in a frequency-hopping receiver, a fixed jammer would have to increase both its bandwidth and power by factor of $1/G_p = N$.

The third type of spread spectrum technique is chirp. Chirp uses a surface acoustical wave (SAW) device to produce a frequency modulated (FM) signal which

increases linearly over the chirp duration time (T). Chirp does not depend on the pseudorandomness characteristics of the wave form like frequency hop and direct spread. Instead it depends on the transfer characteristics of the SAW device. One result of chirp is that all frequency components arrive at the output of the SAW device at the same time, are added, and produce an output proportional to the inverse of the bandwidth.⁴⁶ The result is a signal which is hard, if not impossible, to reduplicate. Hence, security is provided above multi-access requirements.

Four significant characteristics result from SS techniques:

1. Multipath fading is eliminated as a major degradation to the system.
2. The strong capture capability of SS enhances the access efficiency and reduces the effects of interference. SSMA allows the user to capture packets, while CDMA permits the user to capture the channel.
3. Spread spectrum allows coexistence with other systems for better spectrum efficiency.
4. Security is enhanced by low probability of intercept, and anti-jamming characteristics, through signal processing.

The capabilities added by SS techniques add a cost to the network. There is additional complexity for equipment and system protocols. Also probably one of the

biggest limitations, is the synchronization problem. Methods for either unsynchronized or code slotted networks must be designed to compensate for the random access transmissions of a packet radio network. This is an involved process of very complex engineering.⁴⁷

Carrier Sense Multiple Access (CSMA)

Carrier sense multiple access has been compared to an early warning system. Unlike the contention based ALOHA, CSMA uses it's early warning senses to detect other terminals that might be transmitting within the network. By listening very closely before sending, CSMA can avoid overlapping packets. It's results offer possibilities of eighty to ninety percent utilization of the channel, with low end-to-end transmission delay per packet. CSMA is one of the more efficient control techniques being tested for the ground radio environment.⁴⁸

There are three types of CSMA protocols available, of which nonpersistent and p-persistent are the most used. They operate as follows:

	Nonpersistent Carrier Sense	Persistent Carrier Sense	p-Persistent Carrier Sense
IF THE CHANNEL IS SENSED IDLE:	The terminal transmits the packet.	The terminal transmits the packet.	With probability p, the terminal transmits the packet. With probability 1-p, the terminal delays for one time slot and starts again.

	Nonpersistent Carrier Sense	Persistent Carrier Sense	p-Persistent Carrier Sense
IF THE CHANNEL IS SENSED BUSY:	The terminal reschedules the trans- mission to a later time slot accord- ing to a re- transmission delay distri- bution. At this time it repeats the algorithm.	The terminal waits until the channel goes idle and then immediately transmits the packet.	The terminal waits until the channel goes idle and then repeats the above algor- ithm. ⁴⁹

Although CSMA relieves the severe contention problems encountered in ALOHA, it still has some deficiencies. In its normal state, known as collision avoidance, CSMA waits until the channel is sensed idle and then transmits. Other nodes in the network are waiting for the same idle condition. Two ready nodes which identified the same idle time and transmitted resulted in a collision. While the collision overlaps two packets, it is not necessary that both be destroyed. By applying a capture effect along with CSMA, one of the packets can be saved. Another state of CSMA is called collision detection. In the same situation where two ready nodes transmit in the same idle time, one of the nodes detects a collision with the other by comparing the bit stream it is transmitting to the bit stream it sees on the channel. The node detecting collision immediately terminates transmission of the packet.⁵⁰ Again, where capture effect can be important

is in the fact that the first packet, which reached it's destination first, was not destroyed by any overlap.

Another more efficient version of CSMA uses slots for additional control of contention. The slots are not used for entire packets, but are based instead on the maximum propagation delay between pairs of nodes. The distinction between slotted ALOHA and slotted CSMA is that transmission time of CSMA is equivalent to several slots, which are referred to as minislots. The ratio of the maximum propagations delay (which is equivalent to the minislot time period, τ) to the packet length is a parameter, "a", which provides estimates of channel throughput. For terrestrial systems, such as packet radio, this value is typically less than one. For a satellite system values range from ten to over one hundred. The value of "a" also determines how CSMA reacts to other traffic on the channel. A value for "a" equals zero means that propagation delay is truly negligible compared to the packet size. The terminal user with this value has perfect knowledge of the channel condition during the time it is listening.⁵¹ This leads to less contention and higher throughput. To accomplish higher throughput, the minislots act as keying for packet transmissions. For p-persistent CSMA protocol, the terminal senses the channel idle, then with probability p, transmits the packet at the beginning of the minislot. For

probability 1-p, the terminal senses the channel idle, and transmits the packet at the completion of the minislot. By using the minislotted version of CSMA, terminals are able to sense the channel within a relevant time (propagation delay). Very accurate sensing is achieved and throughput is increased significantly.⁵²

There are carrier sense strategies which improve the likelihood of successfully transmitting and receiving packets. This is particularly important in an environment which is hostile, such as encountered by the military. Capture effect, for example, is an alternate means of dealing with contention. This can be achieved by several methods, one of which is through FM modulated circuits which can discriminate between weak and strong signals and reject the weaker signals. The ultimate version would be a slotted CSMA protocol in which all slots can be individually discriminated from every other slot in the receiver. The sensitivity of discrimination implied by this goal is not achievable by today's standard (one hundred percent), but a reasonable goal in the near future might be fifty percent.⁵³

Another widely theorized carrier sense strategy uses spread spectrum techniques for packet capture. In the discussion of SSMA, one of the significant characteristics of SS is its strong capture capability. Early models of carrier sense predicted that a packet radio could either sense in-band RF energy, or in-lock status

indications received from the synchronizing circuitry. But in a tactical crisis, either method may suffer false sensing due to the high interference environment. The repetitive use of the same synchronizing waveform also allows a jammer to identify the means to tie up the system with bogey packets. A code slotted system, on the other hand, eliminates false sensing problems, since a new waveform is used in each slot. The code slotted system would be responsible for sensing the preamble portion of the packet. All other portions of the packet are rejected if not received with a properly coded preamble. This provides a capture effect to occur, since subsequent preambles are missed while the terminal is accepting any given packet.⁵⁴

In conclusion, the sensing strategies for CSMA continue to receive attention from military planners. They offer the advantages of an uncontrolled access method, while providing improved performance. Under stringent ECCM requirements, CSMA may be rejected as a stand-alone multiaccess protocol. But in more complex combined strategies, CSMA proves to be extremely efficient and offers advantages in ECCM protection. In a tailored strategy called minislotted alternating priorities (MSAP), polling with distributed control was accomplished by carrier sensing. One solution for better per-

formance in the multihop environment was achieved by combining MSAP with the use of the busy tone concept, both of which employed the carrier sense strategy.⁵⁵

NOTES, CHAPTER 4

¹ W.R. Franta and Imrich Chlamtac, Local Networks, Lexington Books, 1981, p. 28.

² H. Zimmerman, "OSI Reference Model--The ISO Model of Architecture for Open Systems Interconnection," IEEE Transactions on Communications, April 1980, pp. 425-432.

³ Andrew S. Tanenbaum, Computer Networks, Prentice-Hall, Inc., 1981, p. 16.

⁴ Vinton G. Cerf and Peter T. Kirstein, "Issues in Packet-Network Interconnection," Proceedings of the IEEE, November 1978, p. 1391.

⁵ James P. Gray and Charles R. Blair, "IBM's Systems Network Architecture," Datamation, April 1975, pp. 51-53.

⁶ Cerf and Kirstein, p. 1390.

⁷ John Tyszko, "New Transmission Media for Local Loop to Reshape Telecommunications," Data Management, vol. 20, no. 4, April 1982, p. 25.

⁸ Richard V. Palermo, "Data in the Fast Lane: Digital Termination System," Satellite Communications, March 1983, p. 23.

⁹ Tanenbaum, pp. 16-19.

¹⁰ Wushow Chou, ed., Computer Communications Volume I Principles, Prentice-Hall, Inc., 1983, pp. 41-46.

¹¹ Ibid., pp. 46-48.

¹² Ibid., pp. 48-50.

¹³ R.F. Sproull and D. Cohen, "High-Level Protocols," Proceedings of the IEEE, November 1978, pp. 1371-1386.

¹⁴S.D. Crocker, J.F. Heafner, R.M. Metcalf, and J.R. Postel, "Function-Oriented Protocols for the ARPA Computer Network," AFIPS Proceedings SJCC, May 1972, pp. 271-279.

¹⁵Chou, pp. 50-53.

¹⁶Ibid., pp. 54-55.

¹⁷Vinton G. Cerf, "DARPA Activities in Packet Network Interconnection," in Interlinking of Computer Networks, ed. K.G. Beauchamp, D. Reidel Publishing Company, 1979, pp. 288-290.

¹⁸L. Pouzin, "A Proposal for Interconnecting Packet Switching Networks," Proceedings of EUROCOMP, May 1974, pp. 1023-1036.

¹⁹Cerf, p. 290.

²⁰Cerf and Kirstein, p. 1393.

²¹Ibid., p. 1394.

²²Tanenbaum, p. 196.

²³L. Pouzin and H. Zimmerman, "A Tutorial on Protocols," Proceedings of IEEE, November 1978, pp. 1346-1370.

²⁴Cerf and Kirstein, pp. 1397-1398.

²⁵Ibid., pp. 1398-1399.

²⁶Roy D. Rosner, Packet Switching, Lifetime Learning Publications, 1982, p. 116.

²⁷Ibid., pp. 112-113.

²⁸Ibid., p. 117.

²⁹Tanenbaum, p. 189.

³⁰Franta, pp. 439-444.

³¹Ibid., pp. 445-446.

³²Cerf and Kirstein, p. 1396.

³³Howard Frank, Israel Gitman and Richard Van Slyke, "Packet Radio System--Network Considerations," AFIPS Conference Proceedings, Anaheim, 1975, p. 223.

³⁴Ibid., p. 223.

- ³⁵Tanenbaum, p. 278.
- ³⁶Robert E. Kahn, Steven A. Gronemeyer, Jerry Burchfiel and Ronald C. Kunzelman, "Advances in Packet Radio Technology," Proceedings of the IEEE, November 1978, p. 1480.
- ³⁷Ibid., p. 1480.
- ³⁸Tanenbaum, pp. 279-280.
- ³⁹Kahn et al., p. 1479.
- ⁴⁰Tanenbaum, p. 281.
- ⁴¹Fouad A. Tobagi, "Multiaccess Protocols in Packet Communication Systems," IEEE Transactions on Communications, April 1980, p. 468.
- ⁴²Ibid., p. 477.
- ⁴³Ibid., p. 477.
- ⁴⁴Marc Spellman, "Spread-Spectrum Radios Thwart Hostile Jammers," Microwaves, September 1981, pp. 85-87.
- ⁴⁵Chou, p. 196.
- ⁴⁶Spellman, pp. 88-89.
- ⁴⁷Kahn et al., p. 1485.
- ⁴⁸Ibid., p. 1476.
- ⁴⁹James Martin, Future Developments in Telecommunications, Prentice-Hall, Inc., 1977, p. 595.
- ⁵⁰Tobagi, pp. 472-473.
- ⁵¹Rosner, pp. 252-254.
- ⁵²Tobagi, p. 472.
- ⁵³Martin, pp. 596-597.
- ⁵⁴Kahn et al., pp. 1487-1488.
- ⁵⁵Fouad A. Tobagi, "Analysis of a Two-Hop Centralized Packet Radio Network-Part II: CSMA," IEEE Transactions on Communications, February 1980, pp. 213-214.

CHAPTER 5

THE EXPERIMENTAL PACKET RADIO

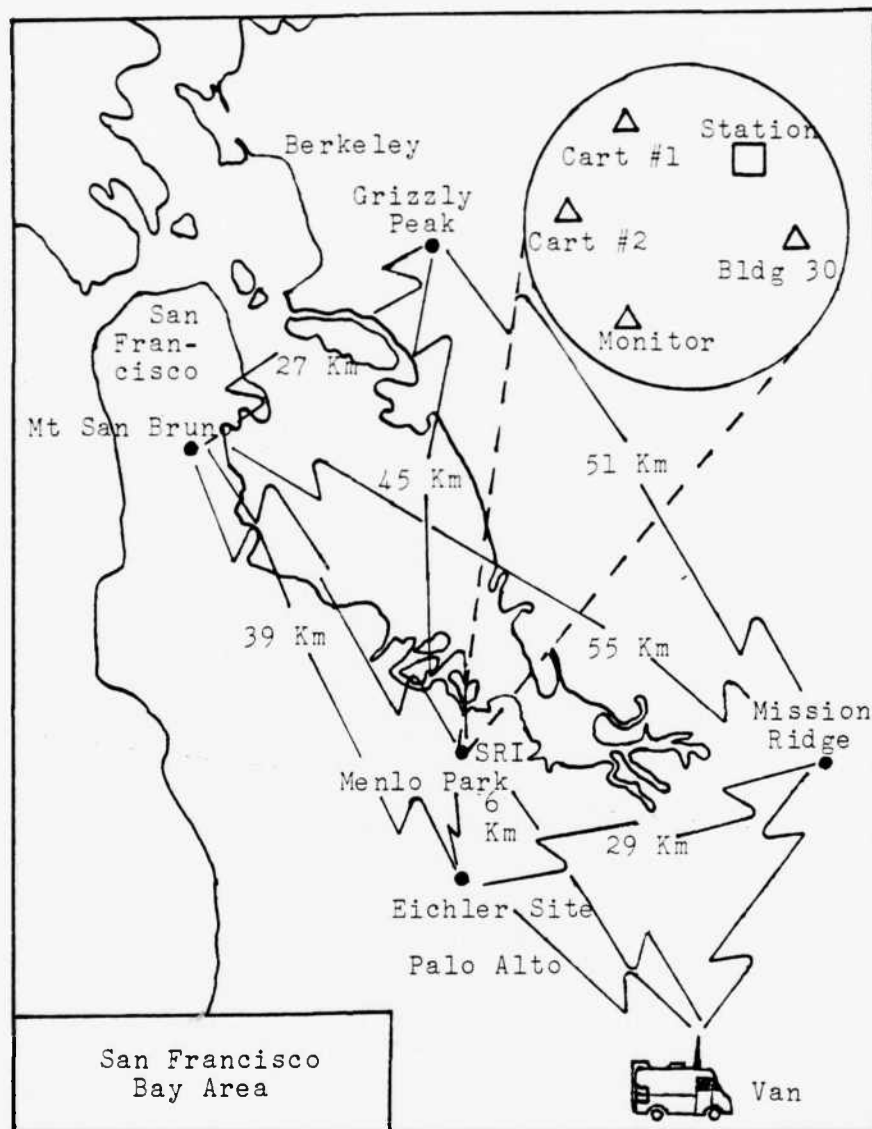
ARPA has been a leader in new packet technology, and on a smaller scale, has fostered testbed programs in many areas of research. One of the most daring programs took form in 1973 with a written draft proposal for an experimental packet radio network. The draft plan called for a group of packet radios to be built and operated for no specific period. It's objectives were as follows:

To develop a geographically distributed network consisting of an array of packet radios managed by one or more mini-computer based stations, and to experimentally evaluate the performance of the system.¹

In mid-1975 the first radios were delivered to the San Francisco Bay area to be operated as a testbed by SRI International, Menlo Park, California. SRI was designated as the System Engineer and Technical Director for the entire operation. The radios were built by Rockwell International and designated as the experimental packet radio (EPR). By September 1976 the network was declared operational with a prototype station software implemented in the network. The quasi-operational network consisted of only twenty-five EPRs, with a goal of fifty radios installed by the end of 1979.²

The SRI experience in the San Francisco Bay area has, since its inception in 1975, gone through extensive testing and changes. Figure 5-1 illustrates the location of the major elements of the packet radio network tested during a 1977 demonstration. The prototype network, made up of EPRs operated both fixed and mobile radios. After only two years of daily operation the network had successfully carried out nearly three dozen major demonstrations.³ The EPR designed by Rockwell International was redesigned into an IPR, improved packet radio, with twice as much digital capacity in the microprocessor. This was further improved to a value-engineered packet radio (VPR), which fit compactly into a suitcase. The final version, designed by Rockwell, was a newer experimentation model containing military implemented protection (from jamming) and a larger RF section.

The experiment by SRI in the San Francisco Bay area was officially closed at the end of September 1983. This has not closed the technology development for packet radio, or applications. SRI is still the System Engineer and Technical Director for a testbed operated at Fort Bragg, North Carolina and Offutt Air Force Base, Nebraska. In addition, Bolt, Beranek and Newman (BBN) are overseeing a smaller packet radio network in the Boston area which is a testbed for military security devices. The programs at Fort Bragg and Boston were experiments



Source: Robert E. Kahn et al., "Advances in Packet Radio Technology," Proceedings of the IEEE, vol. 66, no. 11, November 1978, p. 1489.

Figure 5-1 Location of Major Elements of the Packet Radio Tested During 1977

operated for the benefit of the United States Army data requirements. The newest program being tested at the Air Force's Strategic Air Command, will employ packet radio technology to support database management requirements for command post operations. Connectivity will be done through packet radio communication techniques to activate new command posts and replicate data information.

DARPA has used the three packet networks, San Francisco, Fort Bragg and Boston for their internetting experiments. Their goals were:

- To develop techniques which permit computers on different networks to communicate
- To develop computer internetting protocols
- To develop an internetwork gateway
- To integrate data, speech, message technology and security across connected networks

The internetting experiments have achieved many of these goals. In San Francisco, the packet radio network successfully operated across ETHERNET, SATNET, and the ARPANET. The ETHERNET achieved this connectivity through the use of encapsulation in a PUP protocol (examined in Chapter 4). The internet protocol (IP), used in the ARPANET, was adapted to handle the transitions within the separate operating networks. IP is an interface protocol used in the packet switching networks. A combination gateway/station was developed through software implementation to the IMPs in the network. The

station (minicomputer) software provided the following functions:

- Network Routing Control
- Network Gateway
- Network Management Facility
- Debugging
- Information Service
- Configuration Control Module

The significance of these software changes (installed in 1977) was that only the network routing control was required to be at the station. All other functions were achievable from separate hosts attached to the packet radio network (PRNET). This provides two major advantages: it permits expansion of the quality and quantity of services and keeps station software small and simple. The overall result is a system with high connectivity and redundancy, and economic replication of PRNET supporting equipment.⁴

The Fort Bragg packet radio network was established in 1978 as a joint DARPA and Army testbed facility. Its objective was to test the capabilities of packet radio systems for meeting the Army's long-term tactical data, computer-communications requirements. The name designated for the experiment was the Army Tactical Data Distribution Testbed (ATDDT). The ATDDT was one of three application testbed programs initiated as a result of the ARPA C³ Program.

The programmed operation of ATDDT began in December 1978 with the transfer of twenty terminals to Fort Bragg to be used as ARPANET nodes. The primary participating unit selected was the XVIII Airborne Corps. Training and familiarization of Army personnel started January 1979, and the first five EPRs were delivered and installed that summer. The objective was to expand this network to twenty-seven radios by March 1980 so that the network could support major field exercises for the Corps.

The Fort Bragg packet radio network cycled through some of the same changes experienced in the San Francisco Bay area. EPRs were initially installed, with a one-for-one replacement by IPRs scheduled for the future. They have also received some of the VPRs, so that their total network now numbers twenty-eight packet radios, the consistency of which includes EPRs, IPRs and VPRs. The network has been able to achieve connectivity through the ARPANET and SATNET. In a major exercise by the Corps, the PRNET connected five networks together through gateways. The networks consisted of the EPRNET, the IPRNET, the hardwire network, a mobile net and the distant PRNET. Although there were only a limited number of radios in each of the PRNETs, the goal was accomplished of internetting them for a total system interoperability. As a consequence of having only a few radios one of the main limitations is the lack of sufficient numbers of radios to load the system down. The supervisors of the

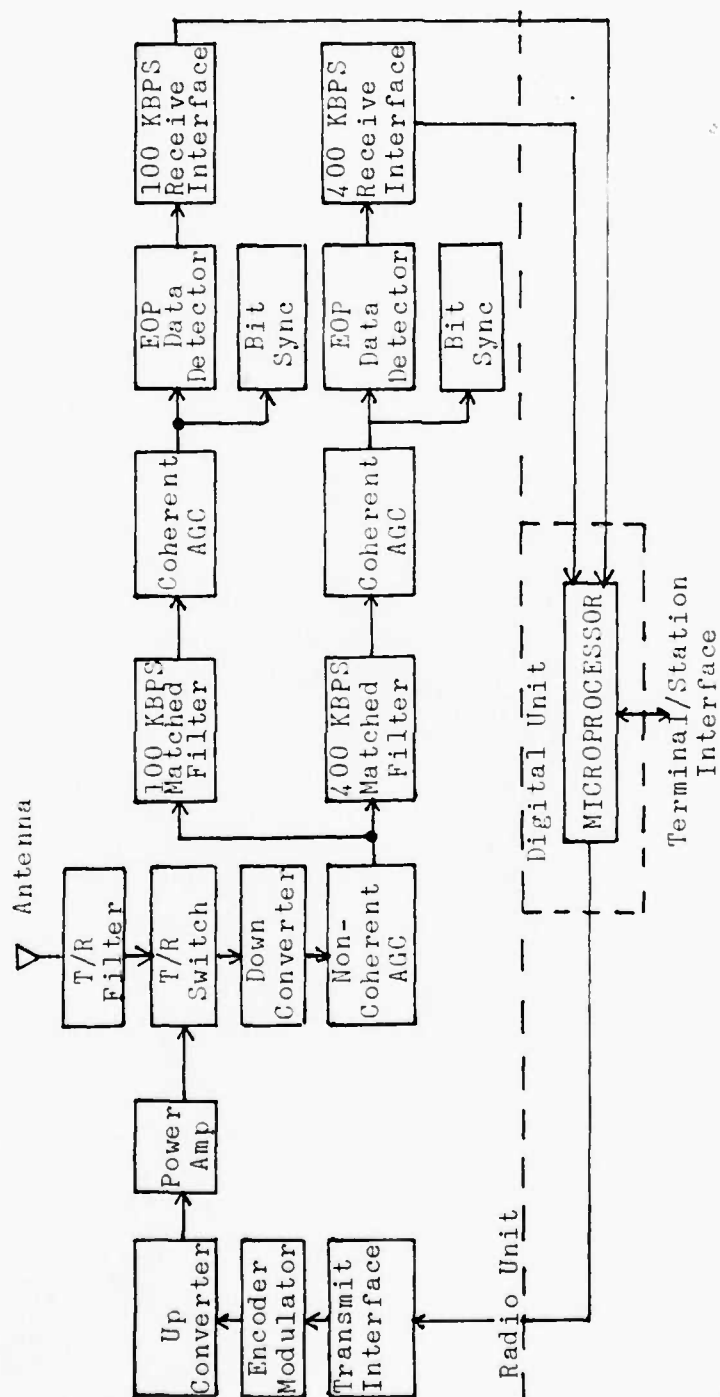
Fort Bragg PRNET were less sure of measurement characteristics due to this major limitation. Statistical analysis has been less accurate and the only way to overcome the deficiency would be by increasing the number of radios.

One of the most significant changes to happen to packet radio was enacted 3 October 1982 on a joint ARPA/Army contract. The contract was signed with the Hazeltine Corporation for \$2.8 million for the low cost packet radio (LCPR). The radios are smaller (420 cubic inches), lighter, require less power and have more capabilities than the existing sets of packet radios. The contract will initially supply one thousand radios by 1986 and includes provisions for an on-going supply of radios for future implementation.

The following sections are devoted to describing the major elements of the EPR development. They are by no means comprehensive, since the EPR has evolved into a number of variations. In addition, no information was available to describe the LCPR under development at Hazeltine. These descriptions are only intended as a guide to major system components.

The Packet Radio Unit

The experimental packet radio (EPR) consists of two basic sections: a radio unit and a microprocessor-based digital unit. Figure 5-2 shows a basic block diagram of the EPR. The radio unit is a RF head which



Source: Robert E. Kahn et al., "Advances in Packet Radio Technology,"
 Proceedings of the IEEE, vol. 66, no. 11, November 1978, p. 1489.

Figure 5-2 Experimental Packet Radio Configuration

transmits and receives packets. The EPR is capable of acting additionally as a repeater. A terminal interface unit, attached to an EPR provides additional multiplexing capability for four terminals. The single portal to the EPR may be connected to a host computer, terminal or station (minicomputer).⁵ The cost for one EPR was \$20,000.

The basic EPR radio unit provides ten watts of output power with a nominal range of twenty miles. The original unit, not hardened, operates from an L-band omnidirectional antenna. The unit operates in a half duplex mode at two data rates, 400 and 100 KPBS. A fixed, direct sequence, pseudo-noise, modulation, (PN) spread spectrum pattern of 128 chips per bit (21 dB processing gain) and 32 chips per bit is respectively applied to the transmission data rates. The slower data rate is only used for links with potentially large multipath spreading. This is because the simpler method of a fixed PN spread spectrum pattern does not provide the ability to discriminate against intersymbol interference. The radio unit performs packet transmissions by adding a 32 bit cyclic redundancy check to the composite packet received from microprocessor memory (ASCII) under direct memory access control. The resultant packet is up-converted to a 20 MHz portion of the 1710-1850 MHz band.⁶

Some encoding is sequentially applied after the packet is formed, but no additional encryption device is used. Packet lengths are variable up to a maximum of 2000 bits.

When not transmitting the EPR remains in a carrier sense receive mode. When a packet is received, the radio unit performs the usual RF head functions (amplification, down-conversion, gain control, etc.). The packet is then put through two parallel operations involving a SAW device with a matched filter, and a differential detector. The two processes are looking for the end of the 100 bit combined preamble/postamble, which when identified, is passed to the microprocessor memory. The microprocessor then determines whether the packet should be relayed, delivered to an attached user or station, or discarded.⁷

The digital unit in the EPR was provided by National Semiconductor with a Model IMP-16 microprocessor. The microprocessor has 4096 16-bit words of random access memory (RAM) and 1024 words of fixed storage (PROM). The network protocols and packet buffers are stored in RAM, and the processor operation system and all input/output routines are contained in PROM. The four basic protocols implemented in the microprocessor are:

- Station to PR Protocol (SPP)
- Channel Access Protocol (CAP)
- CUMSTATS (a statistics gathering feature)
- XRAY (a debugging package)

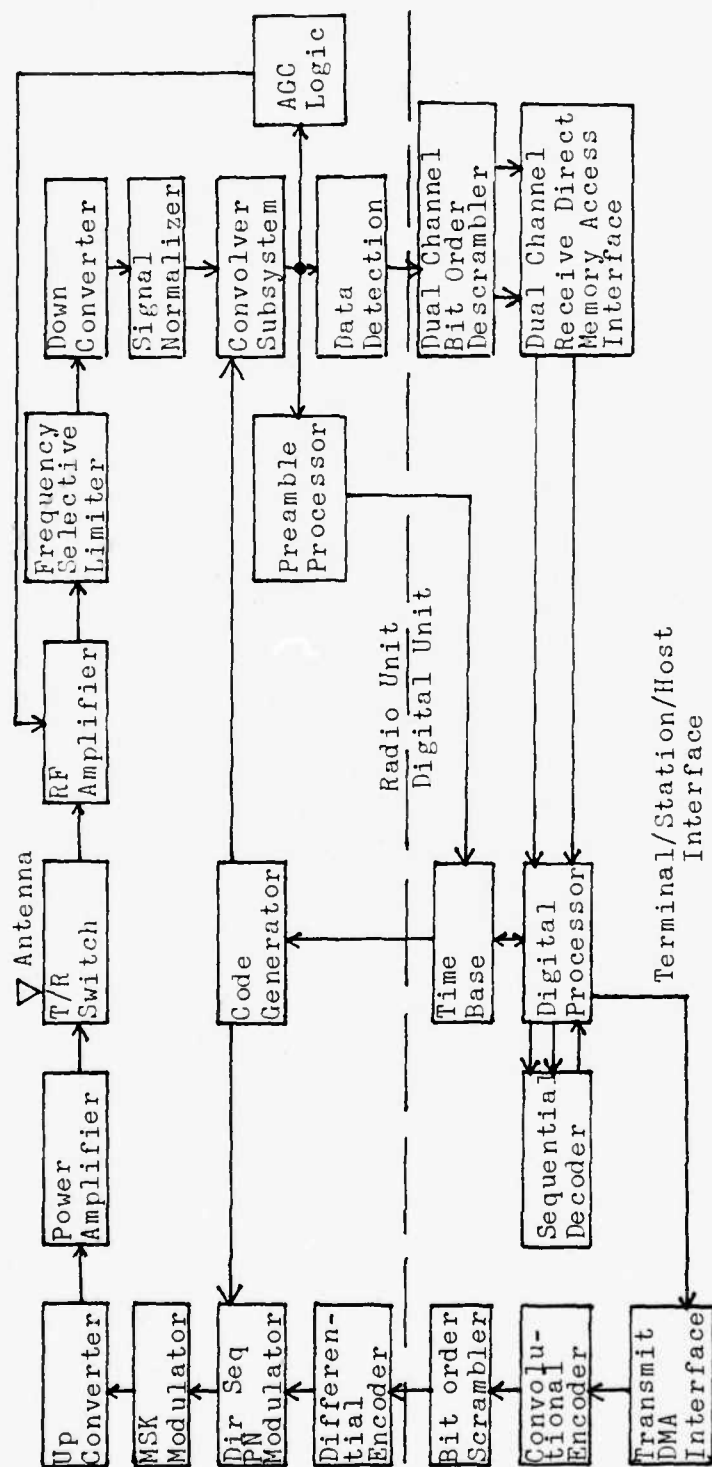
The SPP protocol provides the end-to-end reliability through delivery of network monitor and control packets. The CAP acts as the interface to the network for all EPRs, and serves to launch all packets in the network. Additional protocol layers above CAP must be applied by the user. The additional protocol layer would be required to move a packet over gateways to other networks.⁸ This study will continue with a discussion of the upgraded packet radio (UPR) unit, since it was designed with the tactical environment in mind.

There are only seventy-three packet radios in existence, all built by Rockwell International. There are twenty-eight EPRs, twenty-eight IPRs, and seventeen assorted packet radios, some of which are VPRs, RPRs and UPRs. The UPR, which is tactically enhanced, exists in only three built models. The goal of the UPR model was to provide enhanced capabilities (ECCM) for a limited number of packet radios to operate in hostile environments and to demonstrate the advantages of packet switching radio networks. Unlike the EPR, which was designed for verification of the majority of packet radio protocols and concepts, the UPR was designed to accomplish much more specialized and sophisticated functions. Some of the improvements included:

- A PN pattern which varies on a bit-by-bit basis to spread spectrum modulate each bit
- Programmable matched filter (convolver) to

- receive the PN modulated waveform
- Timing by means of an accurate time of day clock
- A higher spread factor (chips per bit)
- Larger bandwidth, 140 MHz
- Forward error correction based on convolutional coding (constant 24 length code) and sequential decoding (in combination with the error detection and retransmission techniques used in EPR)
- Slotted and nonslotted transmission capability
- Reception of two successive packets with minimum interpacket arrival time
- Low probability of intercept
- Position location capabilities⁹

The UPR was fundamentally changed from the EPR by the use of a direct sequence spread spectrum waveform which varied from bit-to-bit. A block diagram of the UPR is illustrated in Figure 5-3. The EPR's fixed PN pattern was not sufficient to protect the system from jamming or spoofing. An autocorrelation study conducted on the fixed PN pattern revealed a distinct vulnerability to smart jamming. The UPR included several features which permitted easy detection and synchronization of the packet, but low cross-correlation to the PN code sequences used to encode bits. The use of CDMA provided support for simultaneous packet transmissions and a capture mechanism for the channel. The equipment was also designed to



Source: Robert E. Kahn et al., "Advances in Packet Radio Technology," Proceedings of the IEEE, vol. 66, no. 11, November 1978, p. 1491.

Figure 5-3 Upgraded Packet Radio Configuration

generate a high chip stream rate at low power, with a time reversibility characteristic, since the convolver reference chip stream is the reverse of the modulator chip stream over a bit. By running the code generator in advance and storing the chips in memory (and reading them in reverse order), a significant savings of power and hardware can be achieved.¹⁰ The reversibility property was provided by constructing the code set from Gold codes.¹¹

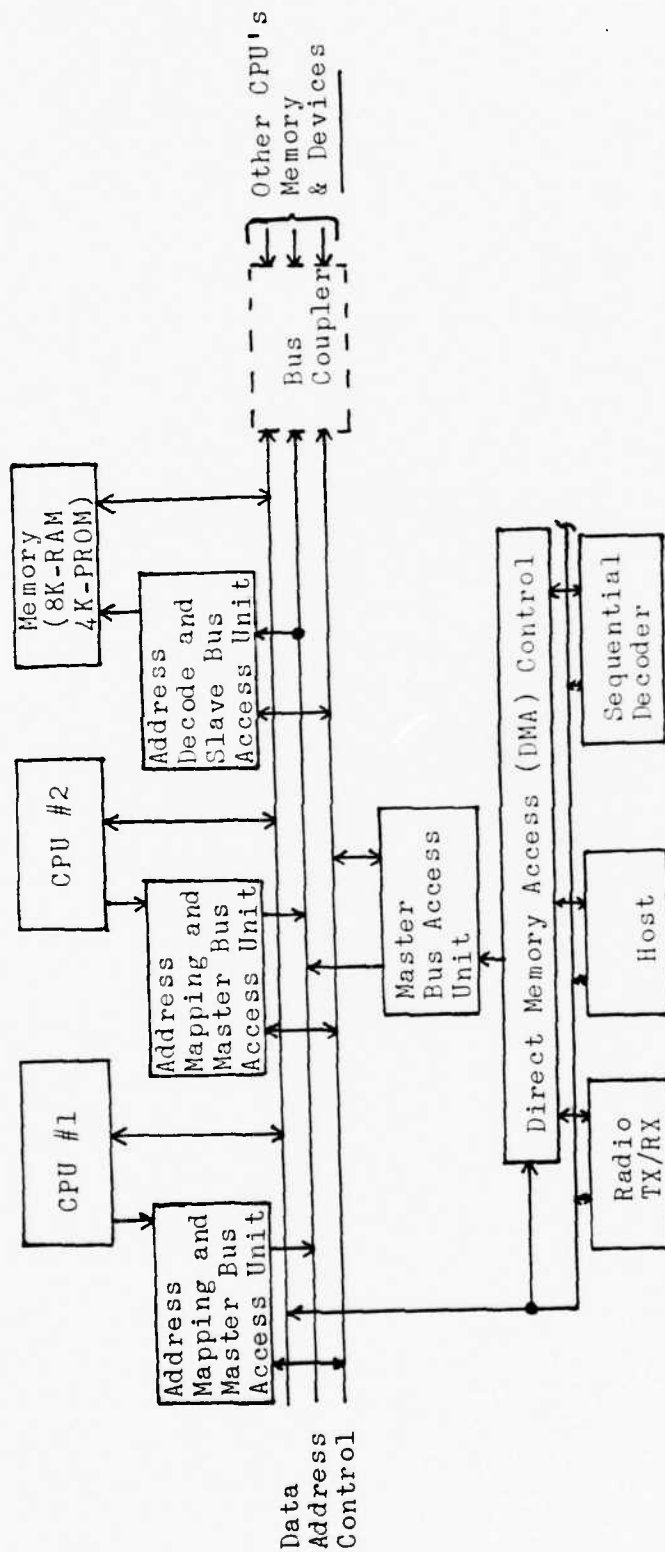
Error control in the UPR was enhanced to include convolutional encoding (block code) with a sequential decoding for forward error correction. This is in addition to the error detection and retransmission techniques used in the EPR. The coding/decoding process is performed only on the header and the text of each packet, and each can be processed at three different speeds of the code generator: $1/4$, $1/2$, and $3/4$ speeds. In addition, the UPR has the capability to decode the header and text separately and at different rates. This permits the operation of the system to decode the headers quickly and protocol process them, while the longer portions of the packet are still being decoded.¹²

The central processor units used by the UPR were changed to Texas Instruments 9900 microprocessors. The processing capabilities of the TI9900 are more powerful, since the added capabilities placed more demands on the

UPR model. Figure 5-4 is a block diagram of the UPR digital section architecture. The processor was also designed to interoperate with the EPR units, which required some dual processor designing.¹³

The UPR was tested in a fixed and a mobile environment. The results of the test showed that the original design parameters were unable to handle the severe fading caused in mobile operations. The cause was attributed primarily to the lock-on procedure used by the UPR to a single multipath component. The velocity of moving caused the UPR to lose its tracking capability of the original locked-on signal. A modification was added through a diversity mechanism based on post-detection integration of multipath components. The modification, even though simple, was so successful that it was added to all other packet radio models.¹⁴

This has been a simple overview of the upgraded packet radio. The experiment, while successfully testing only three working models, has provided extremely outstanding results. The UPR made use of the lessons provided in the EPR experiment, added newer more advanced capabilities, and on its own operation answered some very key questions basic to this study. The EPR and its variations were also very instrumental in the experimental analysis of a packet radio network. Between the two, they provided evidence that a practical military packet radio can be extremely valuable.



Source: Robert E. Kahn et al., "Advances in Packet Radio Technology," Proceedings of the IEEE, vol. 66, no. 11, November 1978, p. 1493.

Figure 5-4 UPR Digital Section Architecture

Network Management and Operation

A centralized network management facility (NMF) similar to ARPANET's network control center was located in the San Francisco Bay area for network monitoring and control. It's primary functions consisted of:

- Debugging by the XRAY protocol
- Testing operational conditions such as power output, frequency, timing and protocol values
- Measurement Experiments
- Fault detection, diagnostics and isolations

The NMF monitors the system using an Interdata 70 computer system, and an EPR to monitor traffic. System monitoring is accomplished by ROPs (radio-on packet), which are periodical broadcasts (every thirty seconds for fixed radios and every five seconds for mobile radios) by individual radios announcing their existence and containing selected status and identification information from the digital unit. The station accumulates these ROPs into tables and status information, and maintains a connectivity matrix based on the information, and from this matrix assigns routes.¹⁵

Packet Radio Repeaters

The repeater is a key device in the PRNET because, through the repeater, the range of terminal-station links can be extended. To accomplish this requirement, repeaters must look like packet radio terminals, while

retaining responsibility and control over their areas of connectivity. The repeater function has been demonstrated in all of the packet radio models, except the VPR model which was designed as a suitcase version. Many of the same design characteristics discussed in the EPR section are applicable to the repeater. While a repeater performs the function of receiving and transmitting packets in the same manner as EPRs, it also must perform routing protocols and error control on the channel as a whole.¹⁶

The radio section of the experimental repeater operates in the simplex mode using two separate RF channels and two independent software programs, making receiving and transmitting modes mutually exclusive. An antenna for the repeater is made up of a four element colinear array. It therefore provides a higher gain (8 dBu) than is possible from the simple whip antenna used by the packet radios.¹⁷

The central processing unit for the repeater is the same National Semiconductor IMP-16 microprocessor (providing a 4 microsecond cycle times) used in the EPRs. The packet transport protocol is provided by the microprocessor to accomplish repeater initialization, packet routing, packet acknowledgements and error control. Using multiprogrammed software, the system was structured into three programs defined as the executive, background and foreground programs. The foreground program handles

packet input/output processes on two levels. A high level packet processing is applied for routing and acknowledgement protocols. A low level packet processing is used for radio and direct memory access control, which performs the actual handling process of packets (under the direction of high level processing). The executive program provides operating system initialization, program control, and system test aids. Finally, the background program provides overlay program, on-line diagnostics, and performance monitoring.¹⁸

The first experimental repeater was built in a 1.23 cubic foot container, weighed forty pounds, and required twenty-five watts of average power. It's primary goal was to add a versatile element to support the packet radio network experiment. A secondary goal was to investigate and demonstrate an application of advanced technology to small, light-weight, self-powered repeaters. From this experiment it was determined that significant savings in size and power can be achieved by using LSI techniques and thin film circuitry. Additionally, it's operation under tactical environments were less than satisfactory, and demanded improvements in processing, antijam and antispoof capability and mobile radio operation.¹⁹ Many of the recommendations in this experiment were carried over to the UPR program and resulted in significant advances in packet radio technology for military applications.

Conclusions

The experimental applications of packet radio have provided successful demonstrations of the basic technology and the security technology. From these examples it is expected that packet radio will most likely play a major role for local distribution of information, particularly when the source or destination can be mobile. The feasibility of the earlier experimental models and progressive improvements, promise packet radio a place in future technology.

NOTES, CHAPTER 5

¹ Robert E. Kahn, Steven A. Gronemeyer, Jerry Burchfiel and Ronald C. Kunzelman, "Advances in Packet Radio Technology," Proceedings of the IEEE, November 1978, p. 1488.

² Ibid., p. 1488.

³ Ibid., p. 1488.

⁴ Ibid., p. 1488.

⁵ Ibid., p. 1490.

⁶ Ibid., p. 1490.

⁷ Ibid., p. 1490.

⁸ Ibid., p. 1490.

⁹ Ibid., pp. 1490-1491.

¹⁰ Ibid., p. 1492.

¹¹ R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing," IEEE Transactions on Information Theory, October 1967, pp. 617-621.

¹² Kahn et al., p. 1492.

¹³ Ibid., pp. 1493-1494.

¹⁴ Ibid., p. 1494.

¹⁵ Ibid., p. 1494.

¹⁶ Stanley C. Fralick and James C. Garrett, "Technological Considerations for Packet Radio Networks," AFIPS Conference Proceedings, Anaheim, 1975, p. 237.

¹⁷ Ibid., p. 238.

¹⁸ Ibid., p. 241.

¹⁹ Ibid., p. 242.

CHAPTER 6

MILITARY APPLICATIONS OF PACKET RADIO

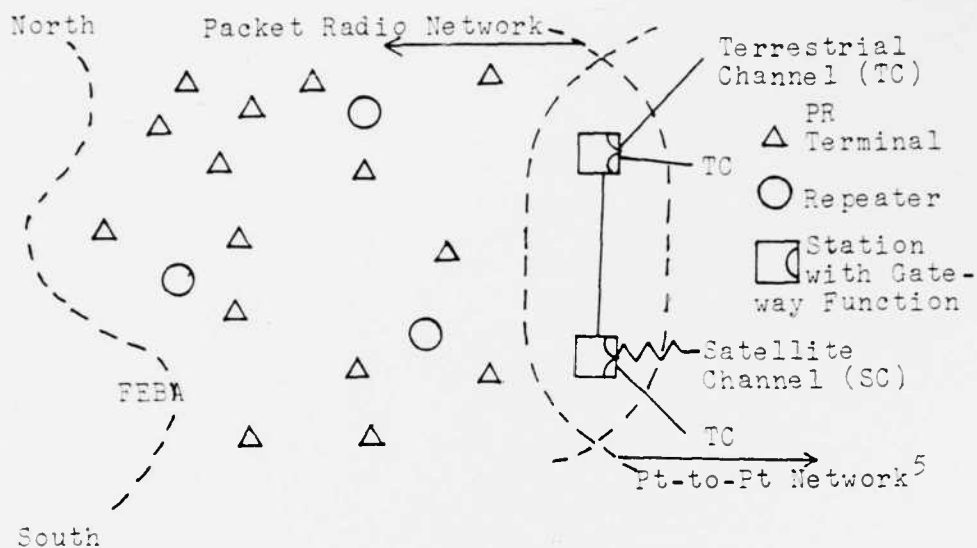
The conceptual model for military applications of packet radio follows (at least) three major situations. The distribution from a central site to remote stations simulates the typical command and control hierarchy of the military, and therefore should be an assumed configuration. Each of the situations in practical use may be illustrated in either stand alone or combined examples, but this will be evident during the discussion. The situations are as follows:

1. The stations are located in areas where the telephone system is poorly developed or nonexistent: nearly all rural areas, and most of the Third World falls into this category. Automated weather and seismic data collection stations are often parachuted into jungles, deserts, and hostile mountain terrain, which frequently lack the amenities of civilization, such as telephone poles.
2. The stations are mobile. A fleet of ships is a good example of a group of users that is inherently mobile. Police cars, ambulances, fire engines, and taxis are other examples.
3. The stations have a high peak-to-average traffic ratio, or a low data rate. In both cases, the cost of a dedicated line may make the application uneconomic. Packet radio offers the possibility of sharing a single channel instead of having a large number of channels with fixed (and mostly wasted) capacity.¹

The emphasis for this discussion focuses entirely on computer communications. A primary objective of a packet radio network is the support of real-time interactive communications between computer resources.² The bulk of the research done in packet radio emphasizes mobile radio communications and computer architecture requirements.³ Terminals attached to the network may range in practical use, to include hand-held devices, teletype-like devices, display devices, computers, and unattended sensors.⁴

Motivation for each of the situations is based on resource sharing of data processing systems. A single channel will be shared by all users generating a need for a scheme to allow multi-access.

The example makes use of a packet radio (PR) network through stations that are highly mobile. The mobility of each station assures the military forces a hasty departure capability in case the forward edge of the battle area (FEBA) is pushed back. It also allows command, control and communications (C³) strategies by upper echelon commanders to be progressively moved to areas most in need. The illustrative description below is used to demonstrate a possible packet radio network configuration:



This network employs three primary functional elements: terminals, stations and repeaters. The terminals permit user interfacing to the network, and the repeaters provide the means to shift terminals outward in order to extend the range for station-terminal links. The FEBA remains fixed temporarily, even though the radios have the capability of communication on the move, so that this discussion can describe the workings of the network. The final element, the station, maintains a rear element position in a management function for the network. All elements are mobile and require little more than mounting/dismounting of the equipment with each move.

The location of this engagement operates in a technically advanced area with an installed backbone of trunking. This has permitted the stations to connect into point-to-point terrestrial lines to allow connect-

ivity to the rear echelon support and C³. One of the stations has established a satellite link through the Defense Satellite Communications System (DSCS). The platform for this satellite connection is also mobile.

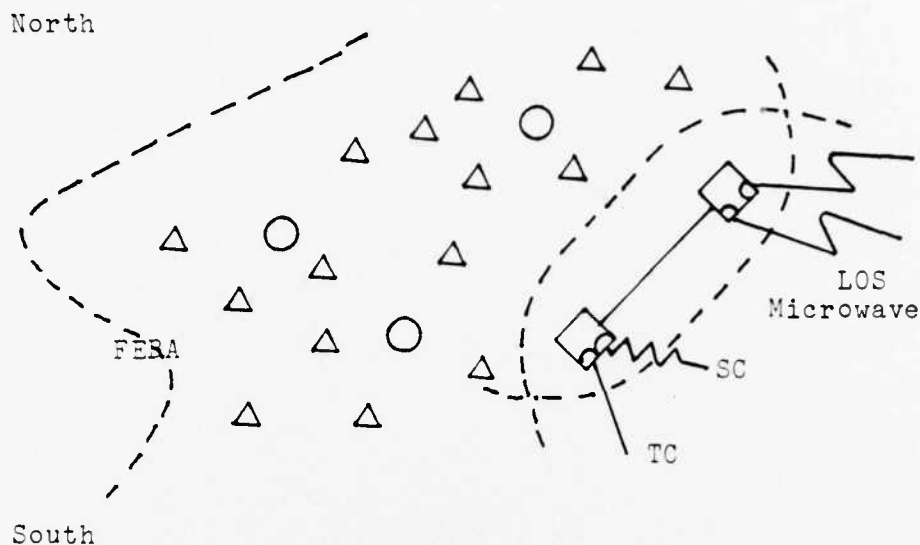
The example is demonstrated in an environment that is hostile. Yet the forces of the enemy threat are incapable of applying interdiction by air forces behind the FEBA. The enemy threat is entirely ground supported using hit and miss tactics and occasional strong confrontations to demonstrate revolutionary strength for the press and newspapers. The stronger confrontations make it necessary to move parts of the network within one hour from notification. Terminals and repeaters are therefore located no closer than thirty-five minutes from the FEBA. All have the capability of rolling at convoy speeds in fifteen minutes or less.

The terminals collect data from front element forces. Some of this data is collected through the voice radio network. Sensors are attached to the mechanized elements, and key forward commanders can send data via hand held devices. The devices are two-way (verification of each transmitted data item is given by a green light on the device) and, besides sending location data at automatic intervals (random), they send varying data for supply, movements, engagements, losses, etc. The use of sensors is a new approach just introduced to the network. One limitation is the fact that sensors have very

limited ranges and many times are not recognized by the repeaters or terminals. The hand held devices on the other hand are recognized by repeaters and terminals more easily due to their higher transmit power.

Our PR network is an overlay to the voice radio network. Experience has demonstrated a capability of the enemy to use jammers and occasionally set up a series of direction finding (DF) stations to key in on major command posts. The detection of jamming has in several cases invoked use of the PR network as a stand-alone system. This also was demonstrated several times when the enemy participated in direction finding to locate key command posts. With voice nets shut down, the efforts of the enemy were invalidated while our forces still maintained communications in the PR network. The bursty nature of the PR network would not permit enemy lock-on to any packet radio transmission. Jamming was less effective on terminals and repeaters, since all used spread spectrum techniques and were able to shut out the erroneous jamming frequencies.

An attack in the north quadrant resulted in the following change to the packet radio network:



The result of the attack in the north quadrant demonstrates the ability of the packet radio network to reconfigure without loss of equipment or communications connectivity. The northern terminals moved away from the FEBA. The dividing line between packet radio networks and point-to-point networks became slanted due to the outbreak of hostilities. The northern station lost temporary connection into the terrestrial trunking network to rear elements, but maintained connectivity via a tropospheric scatter communication system. A station-to-station connection was still available via land line, but could have been supplied in a similar manner as was done with the station to rear elements connections.

This same situation, mobility emphasized, could apply very aptly to a group of ships in the Navy. Requirements for data transfer between battle elements of a naval fleet may fit this situation very closely. A

packet radio network permits ships to forage forward, backward and sideways while maintaining connectivity in the network, either from the ship itself or by airborne repeaters. The difference lies in the changing connectivity required for naval vessels, so ships, must act as repeaters and terminals simultaneously by design. A hierarchical network is less desirable and may require that ships change the role of station or that network management may rely on several ships in coordination with each other.

The mobility emphasized situation in poorly developed areas fits the requirements for a marine assault. The assault group acts as a communication protraction from the main fleet of ships. Element commanders on the front line equipped with a hand held device could be relayed from a beach located repeater to the naval commander. Constant updates of marine locations serve to direct air support or ship bombardment support as the FEBA changes. Front line commanders can relay information of supplies, men and additional materials required to maintain the efforts of the assault. Decisions by naval commanders are enhanced by the capability of contact to the man at the very front of the attack. A commander to fox-hole communication system is provided by the packet radio network. A two-way hand

held device allows direction of the attack personnel from commanders on the ships as well. Mapping of the battle becomes a reality and truly command decisions based on actual combat reaches the overall naval commander as never before.

A concept being developed by the Air Force deviates from this idea that packet radio supports only tactical situations. Aircraft acting as flying repeaters for a strategic data management network permits the command, control and communications of key weapon systems to be air mobile. Ground communications, which are more susceptible to interdiction, can be eliminated in favor of the air mobile platform. Losses of sites or aircraft can be replaced by replicated transfer of database information to newly activated command centers. Packet radio ranges are approximately increased proportionally to the sum of the square roots of the altitude of the aircraft flying as repeater (terminal or station) and the ground radio component. Networks can dynamically rearrange themselves in patterned flights, such as circles, or unpatterned flights to provide unpredictable configurations to possible enemy interceptor aircraft. This type of packet radio network may also support ground forces in tactical maneuvers. The possibilities for an air lifted packet radio network are very diversified and may offer some promising future applications to the military.

As an opportunity for the 1990s, packet radio can be applied by all the military services. The Army has had the most experience with packet radio technology, and could serve as a focal point for future system applications. Packet radio is a promising system approach that can be advanced by the new technologies in LSI/VLSI memories, SAW devices, and microprocessors. Through these advances, military applications of packet radio can offer a more viable communications technique for the mobile data arena.

NOTES, CHAPTER 6

¹ Andrew S. Tanenbaum, Computer Networks, Prentice-Hall, Inc., 1981, p. 277.

² Robert E. Kahn, Steven A. Gronemeyer, Jerry Burchfiel and Ronald C. Kunzelman, "Advances in Packet Radio Technology," Proceedings of the IEEE, November 1978, p. 1469.

³ Robert E. Kahn, "The Organization of Computer Resources into a Packet Radio Network," IEEE Transactions on Communications, January 1977, p. 169.

⁴ Stanley C. Fralick and James C. Garrett, "Technological Considerations for Packet Radio Networks," AFIPS Conference Proceedings, Anaheim, 1975, p. 233.

⁵ Ibid., p. 234.

CHAPTER 7

CONCLUSION

After a decade of designing, testing and experimenting with packet radio, the military has reached a point where they can either advance or stop further consideration of the technology. The investment so far has been in purely research and development phases with less than one hundred packet radio units in operation. Applications have for the most part been limited to army tactical data, computer communications requirements with some off-shoot considerations by the navy and the air force. ARPA has primarily served as the driving force behind packet radio, mainly because they have seen a need to extend the advantages of packet switching to the local mobility arena. Packet radio fills in their gap for local distribution, whereas satellites have taken the major role for long distance distribution. This is also a point in time which is crucial to packet radio, because of the recent plans to make the ARPANET a common-user data network for the military. The decisions, which will eventually establish the Defense Data Network, will have an impact on future packet radio interoperability.

This study has provided an overview of the basic considerations which technically impact the packet radio network. DARPA's experiments in ALOHANET and packet satellite, and other commercial applications in DTS have provided the means through which packet radio has been given a good basic technological head start. ALOHANET, established as an experimental model, has provided test results and design enhancements which were useful in designing the three basic elements of the original packet radio network. It has also served as an operational system fulfilling a real need in computer communications and providing evidence for applications to many devices and network interconnections. The DTS demonstrates that commercial systems are feasible and economically achievable. An established technology base in the packet communications medium enhances the military's ability to find systems that provide working models in other than experimental stages. As the number of sources of packet technology increase so does the knowledge which removes deficiencies, and a corresponding decrease is achieved in costs, which makes the technology more affordable.

Logically, it is imperative that the military provide exact requirements for a packet radio network, to include those attributes which most favor their environment. A well designed system takes into account all advantages and disadvantages, looks at major elements of

the system which might be improved, and recognizes the technology that it must use and the interface it will have with that technology. A thorough evaluation of all technological considerations was therefore required before reviewing the system.

Most important to this discussion was the protocol requirements. A packet radio system can suitably fit into some protocol models better than others, but all must be considered so that applications are not limited. The four most important topics were identified as the level of interconnection, datagram service, routing and multiple access techniques. Sifting through the maze of choices revealed that packet radio was best served by a datagram service and could effectively operate with a broadcast or a point-to-point routing strategy. In addition, packet radio in a military environment was favorable to a combination of carrier sense and spread spectrum techniques.

The new digital service, which packet radio offers, was demonstrated by the experimental packet radio and subsequent model improvements. For the military to operate in a hostile environment, the upgraded packet radio best serves as an example. While there are many unresolved questions, the upgraded packet radio placed the military's use of packet radio in perspective, so that evaluation was real and not simulated. The models designed by Rockwell International suitably met or exceeded the

requirements for a network, and a subsequent modification proved it could be reliably operated at ground speeds. This achievement alone promises a future for packet radio.

Finally the three situations a packet radio network best fits was demonstrated in a mock setup. While the situation described might be limited, it graphically displays applications and off-shoot applications which favor a packet radio technology for the military.

The use by the military of packet radio depends on the technological advances that will occur over the next five to ten years. The current communications systems used by the military are deficient in their capability to communicate data, vulnerable to ECM, have serious interoperability problems, have high probabilities of enemy interception, and lack a real-time mobility capability. Packet radio on the other hand can fulfill each of these deficiencies and provide the needed technology, cost effectively. The military is becoming more serious about packet radio. The \$2.8 million contract for a thousand packet radios is sufficient evidence to that statement, and the recent interest by the Air Force's Strategic Air Command proves that the Army is not the only service considering its use. Therefore a practical military packet radio network is approaching the reality stages, and no longer just an experiment.

BIBLIOGRAPHY

- Abramson, Norman, "The Throughput of Packet Broadcasting Channels," IEEE Transactions on Communications, vol. COM-25, no. 1, January 1977, pp. 117-128.
- Bellamy, John C., Digital Telephony, New York: John Wiley and Sons, 1982.
- Binder, R., W.S. Lai and M. Wilson, "The ALOHANET Menehune-Version II," ALOHA System Technical Report B 74-6, University of Hawaii, September 1974.
- Binder, R., N. Abramson, F. Kuo and D. Wax, "ALOHA Packet Broadcasting--A Retrospect," AFIPS Conference Proceedings, vol. 44, 1975 NCC, Anaheim, pp. 203-215.
- Cerf, Vinton G., "DARPA Activities in Packet Network Interconnection," In Interlinking of Computer Networks, Ed. K.G. Beauchamp, Dordrecht: D. Reidel Publishing Company, 1979.
- Cerf, Vinton G. and Peter T. Kirstein, "Issues in Packet-Network Interconnection," Proceedings of the IEEE, vol. 66, no. 11, November 1978, pp. 1386-1407.
- Chou, Wushow, ed., Computer Communications Volume I Principles, Englewood Cliffs: Prentice-Hall, Inc., 1983.
- Communications Standard Dictionary, S.v. "antenna," "data-circuit terminating equipment," "data sink," and "data terminal equipment."
- Crocker, S.D., J.F. Heafner, R.M. Metcalf and J.R. Postel, "Function-Oriented Protocols for the ARPA Computer Network," AFIPS Proceedings SJCC, vol. 40, 1972, Atlantic City, pp. 271-279.
- Fralick, Stanley C., David H. Brandin, "Digital Terminals for Packet Broadcasting," AFIPS Conference Proceedings, vol. 44, 1975 NCC, Anaheim, pp. 253-261.
- Fralick, Stanley C. and James C. Garrett, "Technological Considerations for Packet Radio Networks," AFIPS Conference Proceedings, vol. 44, 1975 NCC, Anaheim, pp. 233-242.

- Frank, Howard, Israel Gitman and Richard Van Slyke, "Packet Radio System--Network Considerations," AFIPS Conference Proceedings, vol. 44, 1975 NCC, Anaheim, pp. 217-230.
- Frank, Ronald A., "Beyond Local Loops," Datamation, vol. 28, no. 4, April 1982, pp. 90-94.
- Franta, W.R. and Imrich Chlamtac, Local Networks, Lexington: Lexington Books, 1981.
- Gold, R., "Optimal Binary Sequences for Spread Spectrum Multiplexing," IEEE Transactions on Information Theory, October 1967, pp. 617-621.
- Gray, James P. and Charles R. Blair, "IBM's Systems Network Architecture," Datamation, April 1975, pp. 51-56.
- Heiden, Heidi B., "Defense Data Network," Fifteenth Annual Electronics and Aerospace Systems Conference, EASCON 1982, Washington D.C., pp. 61-75.
- Kahn, Robert E., "The Organization of Computer Resources into a Packet Radio Network," IEEE Transactions on Communications, vol. COM-25, no. 1, January 1977, pp. 169-177.
- Kahn, Robert E., Steven A. Gronemeyer, Jerry Burchfiel and Ronald C. Kunzelman, "Advances in Packet Radio Technology," Proceedings of the IEEE, vol. 66, no. 11, November 1978, pp. 1468-1495.
- Kleinrock, Leonard, "Principles and Lessons in Packet Communications," Proceedings of the IEEE, vol. 66 no. 11, November 1978, pp. 1320-1329.
- Kuo, Franklin F., "Defense Packet Switching Networks in the United States," In Interlinking of Computer Networks, Ed. K.G. Beauchamp, Dordrecht: D. Reidel Publishing Company, 1979.
- Kuo, Franklin F., "Panel on Military Data Networks: Present Plans and Future Requirements," Sixth Data Communications Symposium, November 1979, Pacific Grove, pp. 226-229.
- Martin, James., Future Developments in Telecommunications, Englewood Cliffs: Prentice-Hall, Inc., 1977.
- Martin, James., Telecommunications and the Computer, Englewood Cliffs: Prentice-Hall, Inc., 1976.

- Palermo, Richard V., "Data in the Fast Lane: Digital Termination System," Satellite Communications, March 1983, pp. 20-26.
- Pouzin, L., "A Proposal for Interconnecting Packet Switching Networks," Proceedings of EUROCOMP, May 1974, pp. 1023-1036.
- Pouzin, L. and H. Zimmerman, "A Tutorial on Protocols," Proceedings of the IEEE, vol. 66, no. 11, November 1978, pp. 1346-1370.
- Rosner, Roy D., Packet Switching, Belmont: Lifetime Learning Publications, 1982.
- Spellman, Marc, "Spread-Spectrum Radios Thwart Hostile Jammers," Microwaves, September 1981, pp. 85-90.
- Sproull, R.F. and D. Cohen, "High-Level Protocols," Proceedings of the IEEE, vol. 66, no. 11, November 1978, pp. 1371-1386.
- Tanenbaum, Andrew S., Computer Networks, Englewood Cliffs: Prentice-Hall, Inc., 1981.
- Tobagi, Fouad A., "Analysis of a Two-Hop Centralized Packet Radio Network--Part II: Carrier Sense Multiple Access," IEEE Transactions on Communications, vol. COM-28, no. 2, February 1980, pp. 208-216.
- Tobagi, Fouad A., "Multiaccess Protocols in Packet Communication Systems," IEEE Transactions on Communications, vol. COM-28, no. 4, April 1980, pp. 468-486.
- Tyszko, John, "New Transmission Media for Local Loop to Reshape Telecommunications," Data Management, vol. 20, no. 4, April 1982, pp. 24-26.
- Zimmerman, H., "OSI Reference Model--The ISO Model of Architecture for Open Systems Interconnection," IEEE Transactions on Communications, vol. COM-28, no. 4, April 1980, pp. 425-432.

LMED
8